Security Mechanisms for Next Generation Mobile IP Networks

Yingli Sheng

Submitted for the Degree of
Doctor of Philosophy from the
University of Surrey

UNIVERSITY OF SURREY
Centre for Communication Systems Research (CCSR)
School of Electronics and Physical Sciences
University of Surrey
Guildford, Surrey GU2 7XH, UK

July 2011

© Yingli Sheng 2011
Abstract

With the advent of various access technologies and increasing number of applications, a set of challenges concerning efficient delivery of ubiquitous services to heterogeneous users and devices have been posed. Mobile IP protocol can be used to enable roaming across different access technologies. One of the important challenges in Mobile IP is security. The service delivery should be secured and efficient, which implicates that security should be integrated with mobility management (MM), Quality-of-Service (QoS) to minimise the negative impact of security mechanisms. It is proposed in the thesis an architectural framework, which uses Hierarchical Mobile IPv6 (HMIPv6) protocols interworking with Authentication, Authorization, Accounting (AAA) framework. The concept of Enhanced Node (EN) is introduced in the framework. The EN is empowered with intelligence to integrate security, MM and QoS. The focal point of the work is to address security challenges based on the framework and to evaluate the impact of security mechanisms on the mobile networks in terms of extra signalling load introduced.

Three security mechanisms are proposed in the thesis, according to the handover domains. For handover across two access networks, an enhanced AAA solution is proposed to provide the mobile node authenticated network access. It establishes keys between serving access network and target access network for the purpose of securing context transfer. Also keys are established between mobile node and the target access network for future use after mobile node (MN) roams to the target access network. For micro-mobility handover within one EN domain, an enhanced key management scheme is proposed to generate a bunch of handover keys for all of the access routers (AR) within one EN domain instead of generating key every single time the mobile node changes the AR in the previous mechanism. The enhanced key management scheme reduces the handover disruption time introduced by security. For fast handovers within one EN domain (micro-mobility handover) and across EN domains (macro-mobility handover), the security mechanism is proposed to secure the fast handover between ARs/ENs. The fast handover key is established between previous AR/EN and new AR/EN, thus, the fast handover registration messages between ARs/ENs can be secured. More importantly, the context transfer messages between previous EN and new EN for the purpose of prompting “smooth handover”, can be protected using the fast handover keys. The performance of three proposed solutions is evaluated using analytical models. Signalling cost is the main parameter to be evaluated. Discussions on advantage and disadvantage of each proposed mechanisms are also provided at the end of chapter 4, 5 and 6 respectively.

Key words: AAA, enhanced node, Mobile IP, security
Acknowledgments

I would like to express my deepest thanks to my supervisor, Dr. Haltham Cruickshank, for his continuous understanding and support throughout the period of my PhD study. His useful suggestions and contributions to this work are very much appreciated.

I would also like to thank the Centre for Communication Systems Research (CCSR) for giving me all the support throughout my research programme.

I also wish to express my special thanks to my families, especially my parents. Although they are thousands miles away in China, their constant encouragement is really important for me. Without you all, it would never have been possible.
# Contents

Abstract ........................................................................................................................................ i

Acknowledgments .......................................................................................................................... ii

Contents ......................................................................................................................................... iii

List of Figures .................................................................................................................................. viii

Glossary of Terms ............................................................................................................................. xii

1 Introduction .................................................................................................................................. 1

1.1 Introduction ................................................................................................................................ 1

1.2 Research Objectives .................................................................................................................. 2

1.3 Thesis Structure ......................................................................................................................... 4

1.4 Main Contributions .................................................................................................................... 5

2 Mobility Management and Security Mechanisms in Next Generation Mobile Networks .......... 8

2.1 Mobility Management in Next Generation Mobile Networks .................................................. 8

2.1.1 Ubiquitous Services over Next Generation Heterogeneous Network .................................. 8

2.1.2 Mobile IP Protocols .............................................................................................................. 11

2.1.2.1 Mobile IPv6 ................................................................................................................... 11

2.1.2.2 Hierarchical Mobile IPv6 ........................................................................................... 12

2.1.2.3 Fast Handover for Mobile IPv6 ................................................................................... 14

2.1.2.4 Integration of HMIPv6 and FMIPv6 .......................................................................... 17

2.1.3 Other Micro-mobility Protocols ......................................................................................... 20

2.2 Security Mechanisms for Mobile IP Networks ....................................................................... 22

2.2.1 Security Techniques ............................................................................................................. 22

2.2.1.1 Concepts of Encryption/Decryption and algorithms ..................................................... 22

2.2.1.2 Security Association ....................................................................................................... 23

2.2.1.3 Message Authentication Code (MAC) ........................................................................ 23

2.2.2 Authentication, Authorization and Accounting (AAA) Architecture and Protocols .......... 24

2.2.2.1 RADIUS protocol ........................................................................................................ 26

2.2.2.2 DIAMETER protocol .................................................................................................... 26
## Contents

2.2.2.3 Integration of AAA and Mobile IP ................................................................. 28
2.2.2.4 IPSec Interaction with AAA Protocols ............................................................. 30

3 Architectural Framework ..................................................................................... 32

3.1 Introduction to the Framework ........................................................................... 32
3.2 Enhanced Node .................................................................................................. 33
  3.2.1 Security Component ...................................................................................... 34
  3.2.2 Mobility Management Component ................................................................. 35
  3.2.3 QoS Component ........................................................................................... 36
  3.2.4 Radio Resource Management and Signalling Components ............................... 36
3.3 Security Threats and Requirements ..................................................................... 37
  3.3.1 Security Threat Analysis .................................................................................. 37
  3.3.2 Security Requirements .................................................................................... 38
    3.3.2.1 General Security Requirements .................................................................. 38
    3.3.2.2 Specific Security Requirements ................................................................. 39

4 An Enhanced Solution for the Authenticated and Authorized Access Control .......... 40

  4.1 Previous work .................................................................................................... 40
  4.2 AAA Architecture and Trust Model ...................................................................... 41
    4.2.1 AAA Architecture and Functionalities ............................................................ 41
    4.2.2 Trust Model for AAA/Mobile IP Application .................................................. 43
      4.2.2.1 Pre-shared Security Association ................................................................. 44
      4.2.2.2 AAA Security Association ......................................................................... 44
      4.2.2.3 Mobility Security Association ................................................................. 45
  4.3 Authenticated and authorized network access mechanism .................................... 45
    4.3.1 Assumptions .................................................................................................. 45
    4.3.2 Description of the Mechanism ....................................................................... 46
    4.3.3 Benefits of the Mechanism .......................................................................... 50
    4.3.4 Compatibility with the localized AAA solution ............................................... 51
  4.4 Syntax and Semantics of the Messages ................................................................ 53
    4.4.1 Protocols Used between Different Network Entities ....................................... 53
    4.4.2 Extensions for Mobile IP Protocol .................................................................. 54
    4.4.3 Extensions for AAA Protocol ......................................................................... 57
  4.5 Analytical Models ............................................................................................... 59
    4.5.1 Network Model ............................................................................................ 59
## Contents

4.5.2 User Mobility Models ............................................................... 60
   4.5.2.1 Fluid flow model ............................................................... 61
   4.5.2.2 Random walk model ......................................................... 62
4.5.3 Calculation of the Signalling Cost .............................................. 63
   4.5.3.1 Signalling Cost Using Fluid Flow Model ................................. 63
   4.5.3.2 Signalling Cost Using Random Walk Model ......................... 66
4.6 Simulation Results and Analysis .................................................. 67
   4.6.1 Results Using Fluid Flow Model ............................................ 67
   4.6.2 Results Using Random Walk Model ........................................ 69
4.7 Discussions ........................................................................... 75
5 An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks .............................................. 76
   5.1 Related Work ........................................................................ 77
   5.2 Solution Overview ................................................................. 79
      5.2.1 Operational Domain and New Terminology ............................... 79
      5.2.2 Trust Model .................................................................... 80
      5.2.3 Assumptions and Requirements ........................................... 81
      5.2.4 Overview on the key generation procedure ............................. 82
   5.3 The Enhanced Key Management Scheme for Securing Handovers in HMIPv6 Networks .................................................. 83
      5.3.1 Description of the Signalling Details ...................................... 83
      5.3.2 Details on Key Derivation .................................................... 86
         5.3.2.1 Derivation of HIK .......................................................... 86
         5.3.2.2 Derivation of HK ........................................................... 87
      5.3.3 Syntax and Semantics of the Messages ................................. 88
         5.3.3.1 Handover Key Request/Response Message ....................... 88
         5.3.3.2 New Mobility Options ................................................... 90
         5.3.3.3 AAA Request/Response Message ................................... 94
   5.4 Analytical Models .................................................................... 96
      5.4.1 Network and Mobility Models ............................................ 96
         5.4.1.1 Fluid flow model .......................................................... 96
         5.4.1.2 Random walk model ...................................................... 103
      5.4.2 Signalling Cost Analysis ...................................................... 107
         5.4.2.1 Mobility Signalling Cost ................................................ 107
         5.4.2.2 Security Signalling Cost ............................................... 109
5.5 Simulation Results ................................................................. 114
  5.5.1 Fluid Flow Model........................................................... 114
  5.5.2 Random Walk Model..................................................... 122
  5.5.2.1 Directional Model ..................................................... 122
  5.5.2.2 Rectangular Model .................................................. 125
  5.5.2.3 Hexagonal Model ..................................................... 127
5.6 Discussions .............................................................................. 128

6 Secure Fast Handovers in HMIPv6 .............................................. 130
  6.1 Integration of HMIPv6 with Fast Handovers......................... 130
  6.2 Security Considerations .................................................... 131
  6.3 Previous work ...................................................................... 132
  6.4 Description of the Mechanism .............................................. 133
    6.4.1 Security Association (SA) model ................................ 133
    6.4.2 Handover between ARs within One Enhanced Node Domain .......................... 134
    6.4.3 Handover between Enhanced Nodes ............................ 138
  6.5 Analytical Models ............................................................... 142
    6.5.1 Network Model ........................................................ 142
    6.5.2 Signalling Cost for Mobility Location Update ................. 143
    6.5.3 Security Signalling Cost ............................................. 147
      6.5.3.1 Handover within One Enhanced Node Domain .......... 147
      6.5.3.2 Handover between Enhanced Node Domains ............ 148
  6.6 Simulation Results ............................................................... 151
  6.7 Discussions .......................................................................... 155

7 Conclusions and Future Work ...................................................... 157
  7.1 Conclusions .......................................................................... 157
  7.2 Future Work .......................................................................... 159

Bibliography ................................................................................ 162

Appendix A: The Combined Mobility and QoS Framework for Inter Access Network Handovers ................................................................. 171

Appendix B: DIAMETER/MIP Application-AMR and AMA Commands ................................................................. 175

Appendix C: Table of Parameters .................................................. 178

Appendix D: Handover Delay Analysis .......................................... 185
Contents

Appendix E: The Combined Mobility and QoS Mechanism for Handovers between Enhanced Nodes ................................................................. 190
Appendix F: Kerberos-based Method to Secure Handovers in HMIPv6 .................................................................................. 192
List of Figures

Figure 1.1 Mobile IP: mobility domains ................................................................. 2
Figure 2.1 Multiple choices at different aspects for Ubiquitous Services [1] .......... 9
Figure 2.2 Mobile IPv6 Domain ............................................................................ 11
Figure 2.3 Hierarchical Mobile IPv6 Domain ......................................................... 14
Figure 2.4 FMIPv6 Scenario .................................................................................. 15
Figure 2.5 Predictive Fast Handover Signalling [7] .............................................. 15
Figure 2.6 Fast Handover between MAPs Scenario [11] ........................................ 18
Figure 2.7 Signalling for Fast Handover between MAPs [12] ............................... 19
Figure 2.8 Integration of HMIPv6 and FMIPv6 ...................................................... 20
Figure 2.9 Fundamental Components of AAA Architecture ............................... 25
Figure 2.10 AAA Model in Mobile IP [33] ............................................................. 28
Figure 3.1 Architectural Framework .................................................................... 33
Figure 3.2 Network Support Sub-layer ................................................................. 33
Figure 3.3 Architecture of the enhanced node [46] .............................................. 34
Figure 3.4 Security functionalities of enhanced node [46] .................................... 35
Figure 3.5 Mobility entity’s interaction with other entities [45] ......................... 35
Figure 3.6 QoS entity’s interaction with other entities [45] .................................. 36
Figure 4.1 AAA Hierarchy .................................................................................... 42
Figure 4.2 Trust model for AAA-HMIP integration ............................................. 43
Figure 4.3 Pre-established trust relationship ......................................................... 46
Figure 4.4 Signalling for the proposed authenticated and authorized network access mechanism 49
Figure 4.5 Extended AAA/HMIPv6 integrated architecture ............................... 52
Figure 4.6 Additional SAs for the extended AAA architecture ......................... 52
Figure 4.7 Protocols between network entities .................................................... 53
Figure 4.8 Network Model: Hexagonal layout. (1) One enhanced node domain consisting of 3 rings of ARs; (2) One access network consisting of 3 ring s of enhanced node domains..... 60
Figure 4.9 State transition diagram for the markov chain model ....................... 62
Figure 4.10 Impact of MN’s speed on total signalling load (fluid flow model) ....... 67
Figure 4.11 Impact of R (size of the access network: number of rings) on signalling load, using fluid flow model. (1) Total signalling cost v.s R; (2) Ratio v.s R, where Ratio= total
signalling cost using proposed security mechanism / total signalling cost using previous
security mechanism................................................................................................................... 68

Figure 4.12 Impact of R (size of the access network: number of rings) on signalling load, using
random walk model. (1) Total signalling cost v.s R; (2) Ratio v.s R, where Ratio= total
signalling cost using proposed security mechanism / total signalling cost using previous
security mechanism................................................................................................................... 69

Figure 4.13 Impact of average residence time in enhanced node domain on total signalling load,
using random walk model. (1) R=3; (2) R=3 and R=15 ............................................................. 70

Figure 4.14 Probability v.s signalling cost, using random walk model. The enhanced node domain
residence time follows Gamma distribution with mean=4 and variance=4, 8 or 16. Size of
network R=3.................................................................................................................................. 72

Figure 4.15 Probability v.s signalling cost (signalling cost/network residence time), using random
walk model. The enhanced node domain residence time follows Gamma distribution with
mean=4 and variance=4, 8 or 16. And the network residence time is derived using enhanced
node domain residence time........................................................................................................... 74

Figure 5.1 Different handoff domains: micromobility level, Macromobility level and network
level.................................................................................................................................................. 76

Figure 5.2 The proposed solution: domain and entities involved ................................................. 79

Figure 5.3 Trust Model .................................................................................................................... 81

Figure 5.4 Overview on the key generation procedure .............................................................. 82

Figure 5.5 Signalling of the enhanced key management scheme for securing the handover process
.......................................................................................................................................................... 85

Figure 5.6 Handover Key Request message format ................................................................. 88

Figure 5.7 Handover Key Response message format .............................................................. 89

Figure 5.8 Nonce mobility option .................................................................................................. 91

Figure 5.9 MAC mobility option [86] ......................................................................................... 92

Figure 5.10 HK mobility option .................................................................................................... 93

Figure 5.11 Network model consisting of two layers of nodes ................................................. 96

Figure 5.12 A continuous-time Markov chain model [68].......................................................... 97

Figure 5.13 Network Model. (1) Grid Network Model, in which cell is labelled by the distance to
the centre cell “0”; (2) Distance between cells with coordinates (x1, y1) and (x2, y2) ................. 103

Figure 5.14 MN’s walk model (1) Directional Walk Model; (2) Rectangular Walk Model; (3)
Hexagonal Walk Model .................................................................................................................. 105

Figure 5.15 State diagram for different random walk models. (1) Directional Model; (2)
Rectangular Model; (3) Hexagonal Model ..................................................................................... 106
Figure 5.16 Signalling cost. (1) HMIPv6-based network domain; (2) HMIPv6-based network with previous security mechanism; (3) HMIPv6 based network with the proposed security mechanism

Figure 5.17 $\varphi K$ as a function of $K$. $\varphi K$ is the number of an MN's movements within a given enhanced node domain.

Figure 5.18 Impact of $r=b/a$ on signalling cost, with HKS located in another domain. Parameters: $N=20$; $v=20$ km/hr; $S=10$ km², HK size (1) 128 bits (2) 256 bits.

Figure 5.19 Impact of $r=b/a$ on signalling cost, with HKS located in another domain. Parameters: $N=20$; HK size=128 bits; $v=5$ or 20 km/hr; $S=10$ km².

Figure 5.20 Impact of MN's average speed $v$ on signalling load, with HKS located in another domain and in the visiting domain ($s=2$ hops away from the enhanced node). Parameters: $N=20$; HK size =128 bits; $S=10$ km²; $r=0.2$.

Figure 5.21 Impact of domain size $N$ on signalling cost, with HKS located in another domain and in the same domain ($s=2$ hops away from the enhanced node). Parameters: $v=20$ km/hr; HK size =256 bits; $S=10$ km²; $r=0.2$.

Figure 5.22 Impact of HK size on signalling cost, (1) HKS located in visiting domain, $S=1, 2, 5$ hops away from the enhanced node; (2) HKS is located in another. Parameters: $N=20$; $v=20$ km/hr; HK size=128 bits.

Figure 5.23 Impact of $rs=b/s$ on signalling load, with HKS located in the visiting domain ($s$ hops away from the enhanced node). Parameters: $N=20$; $b=10$; HK size=128 bits.

Figure 5.24 Impact of $r=b/a$ and $rs=b/s$ on $R=\frac{Security\ Signalling}{(HMIP\ Signalling + Security\ Signalling)}$, with HKS located in visiting domain ($s$ hops away from the enhanced node). (1) Previous security mechanism; (2) Proposed security mechanism. Parameters: $N=20$; HK size=128; $v=20$ km/hr; $S=10$ km²; $b=10$.

Figure 5.25 Signalling cost in directional walk model. (1) registration cost in HMIPv6; (2) total signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. $K$ is the distance between HA and enhanced node.

Figure 5.26 Impact of threshold ($d$) on cost ratio in directional walk model. The ratio is defined as: total signalling cost in HMIPv6 with security/ registration cost in HMIPv6.

Figure 5.27 Signalling cost in rectangular walk model. (1) registration cost in HMIPv6; (2) signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. $K$ is the distance between HA and enhanced node.
List of Figures

Figure 5.28  Impact of threshold (d) on cost ratio in rectangular model. The ratio is defined as: total signalling cost in HMIPv6 with security/registration cost in HMIPv6. .......................... 126
Figure 5.29 Signalling cost in hexagonal random walk model. (1) registration cost in HMIPv6; (2) signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. K is the distance between HA and enhanced node. ......................................................................................................................... 127
Figure 5.30 Impact of threshold (d) on cost ratio in hexagonal walk model. The ratio is defined as: total signalling cost in HMIPv6 with security/registration cost in HMIPv6. .................. 128

Figure 6.1 Integration of HMIPv6 and fast handovers ................................................................. 131
Figure 6.2 Trust model for F-HMIPv6 domain ............................................................................ 133
Figure 6.3 Signalling for handover within one enhanced node domain ............................................ 135
Figure 6.4 FBU message format [7] .................................................................................. 135
Figure 6.5 Fast handover key request message ............................................................................ 136
Figure 6.6 Fast handover key response message ........................................................................... 137
Figure 6.7 FHK mobility option .................................................................................................. 137
Figure 6.8 Signalling for handover between enhanced nodes ....................................................... 141
Figure 6.9 The Network Model and handover scenarios, with N=4 and k=3 ................................ 143
Figure 6.10 Signalling cost for location update and security. (1) fast handover between ARs within one enhanced node domain; (2) fast handover between enhanced nodes. .......... 147
Figure 6.11 Probability vs. number of ARs crossed between two consecutive packet arrivals. tc follows exponential distribution with $\lambda c=3$, and $tm$ follows Gamma distribution with varying $\gamma$ and $\lambda m=30$. (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$; (4) $\gamma=10$. .......................................................... 151
Figure 6.12 Signalling cost v.s number of ARs crossed between two consecutive packet arrivals. Tc follows exponential distribution with $\lambda c=3$, and $Tm$ follows Gamma distribution with varying $\gamma$ and $\lambda m=30$. (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$; (4) $\gamma=10$. .......................................................... 152
Figure 6.13 Probability v.s number of ARs crossed between two consecutive packet arrivals. Tc follows Erlang distribution with $\lambda c=3$ and $m=2$. $Tm$ follows Gamma distribution with $\lambda m=30$ and varying $\gamma$ values: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$; (4) $\gamma=10$. .......................................................... 153
Figure 6.14 Signalling cost (LU cost and LU+security cost) v.s number of ARs crossed between two consecutive packet arrivals. Tc follows Erlang distribution with $\lambda c=3$ and $m=2$. $Tm$ follows Gamma distribution with $\lambda m=30$ and varying $\gamma$ values: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$; (4) $\gamma=10$. .......................................................... 153
Figure 6.15 Signalling cost v.s call to mobility ratio $p=\lambda c/\lambda m$. Tc follows Erlang distribution with $m=2$ and $Tm$ follows Gamma distribution with $\gamma=0.1$. .......................................................... 155
# Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, Accounting</td>
</tr>
<tr>
<td>AAAF</td>
<td>AAA Server in Foreign Network</td>
</tr>
<tr>
<td>AAAH</td>
<td>AAA Server in Home Network</td>
</tr>
<tr>
<td>AAAL</td>
<td>Local AAA Server</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header Protocol</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>AR</td>
<td>Access Router</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute Value Pair</td>
</tr>
<tr>
<td>BA</td>
<td>Binding Acknowledgement</td>
</tr>
<tr>
<td>BR</td>
<td>Binding Refresh Request</td>
</tr>
<tr>
<td>BU</td>
<td>Binding Update</td>
</tr>
<tr>
<td>CGA</td>
<td>Cryptographically Generated Address</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CN</td>
<td>Corresponding Node</td>
</tr>
<tr>
<td>CoA</td>
<td>Care-of-Address</td>
</tr>
<tr>
<td>CXTP</td>
<td>Context Transfer Protocol</td>
</tr>
<tr>
<td>(3) DES</td>
<td>(Triple) Data Encryption Standard</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-Service</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EN</td>
<td>Enhanced Node</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload Protocol</td>
</tr>
<tr>
<td>FA</td>
<td>Foreign Agent</td>
</tr>
<tr>
<td>FBA</td>
<td>Fast Binding Acknowledgement</td>
</tr>
<tr>
<td>FBU</td>
<td>Fast Binding Update</td>
</tr>
<tr>
<td>FNA</td>
<td>Fast Neighbour Advertisement</td>
</tr>
<tr>
<td>FMIPv6</td>
<td>Fast Handover Mobile IPv6</td>
</tr>
<tr>
<td>FHMIPv6</td>
<td>Fast Handover for Hierarchical Mobile IPv6</td>
</tr>
<tr>
<td>GW</td>
<td>Gateway</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>Hack</td>
<td>Handover Acknowledgement</td>
</tr>
</tbody>
</table>
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HI</td>
<td>Handover Initiation</td>
</tr>
<tr>
<td>HIK</td>
<td>Handover Integrity Key</td>
</tr>
<tr>
<td>HK</td>
<td>Handover Key</td>
</tr>
<tr>
<td>HKS</td>
<td>Handover Key Server</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash-based Message Authentication Code</td>
</tr>
<tr>
<td>HMIPv6</td>
<td>Hierarchical Mobile IPv6</td>
</tr>
<tr>
<td>HMK</td>
<td>Handover Master Key</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IID</td>
<td>Independent and Identically Distributed</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>KEK</td>
<td>Key Encryption Key</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LCoA</td>
<td>On-Link Care-of-Address</td>
</tr>
<tr>
<td>LSA</td>
<td>Local Security Association</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobility Anchor Point</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-In-The-Middle</td>
</tr>
<tr>
<td>MIPv4/v6</td>
<td>Mobile IPv4/v6</td>
</tr>
<tr>
<td>MM</td>
<td>Mobility Management</td>
</tr>
<tr>
<td>MN</td>
<td>Mobile Node</td>
</tr>
<tr>
<td>NAI</td>
<td>Network Access Identifier</td>
</tr>
<tr>
<td>NAR</td>
<td>New Access Router</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Access Server</td>
</tr>
<tr>
<td>NCoA</td>
<td>New Care-of-Address</td>
</tr>
<tr>
<td>NEN</td>
<td>New Enhanced Node</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NMAP</td>
<td>New Mobility Anchor Point</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAR</td>
<td>Previous Access Router</td>
</tr>
<tr>
<td>PCoA</td>
<td>Previous Care-of-Address</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Density Function</td>
</tr>
<tr>
<td>PDSN</td>
<td>Packet Data Serving Node</td>
</tr>
<tr>
<td>PEN</td>
<td>Previous Enhanced Node</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>PMAP</td>
<td>Previous Mobility Anchor Point</td>
</tr>
<tr>
<td>PMIPv6</td>
<td>Proxy Mobile IPv6</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PRF</td>
<td>Pseudo Random Function</td>
</tr>
<tr>
<td>PrRtAdv.</td>
<td>Proxy Router Advertisement</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RA</td>
<td>Router Advertisement</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RCoA</td>
<td>Regional Care-of-Address</td>
</tr>
<tr>
<td>RRM</td>
<td>Radio Resource Management</td>
</tr>
<tr>
<td>RRT</td>
<td>Round-Trip-Time</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir and Adleman Algorithm</td>
</tr>
<tr>
<td>RtSolPr.</td>
<td>Router Solicitation for Proxy Advertisement</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SEND</td>
<td>Secure Neighbour Discovery Protocol</td>
</tr>
<tr>
<td>SPI</td>
<td>Security Parameter Index</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra-Wideband</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
</tbody>
</table>
Chapter 1

1 Introduction

1.1 Introduction

Delivering ubiquitous services to various mobile users through heterogeneous networks is a major objective in the next generation mobile networks. However, the delivery of ubiquitous services today poses many challenges for the operator. Among various issues, there are three key factors which draw to the attention of many researchers worldwide: Mobility Management (MM), Quality-of-Service (QoS) and security. The service delivery should be efficient and secure. Therefore, the need for secured and seamless fast handovers and the support for the integration of security, QoS and mobility management become parts of the essential issues.

The Internet Engineering Task Force (IETF) made a great effort to propose mobility protocols to enable moving end users and moving networks. Mobile IPv4/v6 protocols and their variations are proposed by IETF to provide the mobile device continuous connectivity while roaming from one network to another. Mobile IP protocols have been implemented in wired and wireless environments where end users need to move across multiple subnets or roam between overlapping wireless systems, such as WiMAX, WLAN, etc. Mobile IP support is also used within CDMA2000 and other cellular systems to provide seamless IP mobility between different packet data serving node (PDSN) domains. Although, Mobile IP is widely proposed to be a wise solution to provide routing services to mobile node that constantly changes its point of attachment to the network, there are many other challenges apart from mobility management. Security and QoS are two of the major ones. In order to deliver the service in a secured and efficient manner, the integration of mobility, security and QoS becomes essential. As research endeavours to improve Mobile IPv4/v6 protocol to achieve better handover performance, in terms of fast, smooth and seamless handovers, it is important that security/QoS mechanism has minimal impact on the handover performance. Thus, providing security solution in Mobile IP requires not only good security design, but also integration with Mobile IP protocol to minimise the overhead, such as extra signalling and delay.

Variations of Mobile IP protocols have been proposed to improve the performance of Mobile IPv6 protocol, such as Hierarchical Mobile IPv6 (HMIPv6), Fast handover Mobile IPv6
(FMIPv6), etc. The research work in the thesis is based on HMIPv6 and FMIPv6 protocols, which will be explained in detail in Chapter 2. There are many security issues existing in Mobile IP which can be summarized as below,

- Authentication/Authorization: The mobile user needs to be authenticated for the network access and to be authorised for the services.
- Efficient key management with minimal overhead: scalable and efficient key management mechanism is essential. With keys/keying materials delivered/established, the mobile IP registration procedure can be secured. And more importantly, the key management scheme should not have too much negative impact on the performance of Mobile IP protocols.
- Anti-replay/Denial-of-Service (DoS) attacks: Among various attacks, replay and DoS attacks are of the most-mentioned ones, which deserve special attention. More explanation of attacks will be provided in section 3.3.

Targeting at solving some of the security issues for HMIPv6 and FMIPv6 based networks, three different security mechanisms are proposed in the thesis. More details regarding the proposed solutions are explained in section 1.2.

1.2 Research Objectives

In order to enhance the handover performance, HMIPv6 and FMIPv6 are proposed by IETF. HMIPv6 provides micro-mobility management enhancement for Mobile IPv6 networks. And FMIPv6 mainly focus on fast handover mechanism. According to handover types, the mobility domains can be classified to three categories as shown in Figure 1.1:

![Figure 1.1 Mobile IP: mobility domains](image-url)
Chapter 1. Introduction

- **Micro-mobility**: secure HMIPv6 mobility signalling (in chapter 5) and fast handover signalling (in chapter 6) for handovers within one mobility agent domain

IP micro mobility usually refers to the mobile communication architecture which is primarily designed to complement the IETF macro-mobility management protocol ‘Mobile IP’. IP micro mobility protocols handle intra-domain (within one mobility agent) mobility of mobile users, without interacting with Mobile IP-enabled Internet to enhance quality of real-time communications, by effectively reducing delay, network overhead and packet loss during handoff. Mobile user performs handover within one mobility agent, as shown in Figure 1.1. The registration procedure is localized within the mobility agent, without the need to traverse the Mobile IP-enabled Internet. Since the registration is performed between the mobile node and the local mobility agent, the registration signalling need to be properly secured. Therefore, the key management mechanism to distribute keys/keying materials between mobility agent, access router and mobile node is required. The key management scheme for securing micro-mobility in HMIPv6 based networks is proposed in chapter 5.

- **Macro-mobility**: secure fast handover signalling for handovers across mobility agent domains (chapter 6)

As opposed to micro-mobility, macro mobility is to handle inter-domain (across mobility agent domains) mobility of mobile users. Mobile IP defines means of providing and managing macro-mobility. However, it introduces large handover latency, packet loss and service degradation. Thus, the fast handover mechanism is introduced to enhance macro-mobility performance, by reducing the handover latency and packet loss rate. The mechanism of context transfer, for instance, QoS context, between neighbouring nodes enhances smooth handover performance which potentially mitigates the degradation of service. It is defined here that the macro-mobility is the mobility level between mobility agent domains within one access network, as shown in Figure 1.1. Thus, providing fast handover mechanism between neighbouring mobility agents are necessary. Meanwhile, the security mechanism to secure the fast handover procedure between mobility agents is required. In the fast handover mechanism, not only registration procedure but also the context transfer/packet forwarding between neighbouring nodes (access router or mobility agent) needs to be secured. Thus, introducing security mechanism to protect registration/context transfer becomes necessary. The mechanism for securing fast handovers in both of micro-mobility and macro-mobility scenarios is proposed in chapter 6.

- **Network-mobility**: authentication of the mobile node, establishing trust between serving and target access networks, distributing security credentials in target access network (chapter 4)
Chapter 1. Introduction

The network-mobility, as shown in Figure 1.1, defines the handover between two access networks. It is actually a special scenario of macro-mobility. And the reason why I separate the macro-mobility between mobility agents and macro-mobility between access networks is that they differ from security point of view, although they look similar from mobility registration perspective. When the mobile node (MN) enters a new access network, it is important that the authentication is performed. And it is also essential that security credentials are distributed in the new access network for future use. Thus, authenticated access control mechanism, which is proposed in chapter 4, is crucial for the network-mobility level.

1.3 Thesis Structure

The rest of the thesis is organized as follow,

Chapter 2 explains Mobile IPv6 protocol in detail, focusing on the location update procedures. Variations of Mobile IPv6, namely HMIPv6, FMIPv6 and the integration of them, are also explained. Other micro-mobility protocols, such as Cellular IP and HAWAII, are mentioned in the end of this chapter and a comparison of common micro-mobility protocols is given. The security techniques and concepts to be used later in the proposed solutions are also explained. A literature survey on Authentication, Authorization and Accounting (AAA) framework and protocols is given, and some initial work on the integration of AAA with Mobile IP is introduced.

Chapter 3 gives an overview of the network architectural framework which the design is based on. The concept of enhanced node, which integrates security, QoS and mobility management, is introduced. Security threat analysis and security design requirements are provided, based on the framework.

Chapter 4 proposes an enhanced AAA solution for authenticated access control, which can be applied for the handover across different access networks (network level mobility shown in Figure 1.1). The proposed mechanism authenticates the mobile node and also establishes security associations between serving and target access networks and between the mobile node and target access networks. The detailed signalling and extensions to Mobile IP and AAA messages are provided. The performance of proposed mechanism is evaluated using analytical models (fluid flow model and random walk model) against the traditional Mobile IP/AAA solution. The signalling overhead introduced by the proposed mechanism is evaluated. The advantage and disadvantage of the proposed solution against the traditional Mobile IP/AAA solution are analyzed.
Chapter 5 proposes an enhanced key management scheme for securing micro-mobility handovers in HMIPv6 based networks. The proposed solution provides an efficient key management scheme by generating a bunch of session keys at one time for all of the access routers within one mobility agent domain. Signalling details and extensions to Mobile IP and AAA messages are explained. The performance of the proposed solution is evaluated using fluid flow and random walk mobility models against the previous mechanism, which generates the session key every time the mobile node performs handovers between access routers. Signalling cost is the main parameter that has been simulated. An analysis of the advantage and disadvantage of the proposed solution against the previous mechanism is provided.

Chapter 6 focuses on security mechanism for fast handovers. It is proposed a solution to secure fast handovers in HMIPv6 based networks. The fast handover here includes micro-mobility level handover, where fast handover is performed between neighbouring access routers, and macro-mobility level handover, where fast handover is performed between neighbouring mobility agents. The proposed solution establishes fast handover keys between previous and new access routers/mobility agents, for the purpose of securing fast handover registration signalling or/and context transfer messages. The performance is evaluated on the parameters of signalling cost introduced by the proposed security mechanism. The total signalling cost with security mechanism enabled is compared to the signalling cost of standard HMIPv6 fast handover protocol.

Finally chapter 7 concludes the thesis by highlighting the outcomes derived from the work and suggests possible directions for future work.

1.4 Main Contributions

The following contributions have been made in this thesis:

1. An enhanced AAA solution for the authenticated access control

The solution is proposed in chapter 4 to secure handovers between different access networks. And it basically enhances the traditional Mobile IP/AAA solution, by providing the mobile MN authenticated access and establishing the security associations in the target access network at the same time. The procedure is performed before the mobile node connects to the target access network, thus, it also mitigates the extra delay introduced by security mechanism.

2. An enhanced key management scheme for securing micro-mobility handovers
Chapter 1. Introduction

The solution is proposed in chapter 5 to secure micro-mobility handovers. It is to establish session keys between mobile node, access router and mobility agent to secure the registration messages exchanged between them. Previously, the session key is generated every time the mobile node changes its point of attachment to the network (access router). The proposed mechanism enhances previous solution by generating a bunch of session keys at one time for all of the access routers within one mobility agent domain, when the mobile node first enters this mobility agent domain. Thus, the handover delay introduced by security mechanism is reduced for any future micro-mobility handovers within this particular mobility agent domain.

3. A solution to secure fast handover in HMIPv6 based networks

The solution is proposed in chapter 6 to secure fast handovers in HMIPv6 based networks. It is basically to establish handover keys between neighbouring access routers/mobility agents, for the purpose of securing registration/context transfer messages. The solution is applied for both of the micro-mobility fast handovers between access routers and the macro-mobility fast handovers between mobility agents.

The integration of HMIPv6 and FMIPv6 protocols is also investigated. The FMIPv6 standard is proposed by IETF for the fast handover between access routers. However, in order to integrate fast handover with HMIPv6, it is even more important that the fast handover between mobility agents can be applied. As the global location update for handover between mobility agents in HMIPv6 can cause even more noticeable delay and packet loss, than handover within mobility agent domain where the location update is localized without the necessity for global update. It is specified in the thesis in section 2.1.2.4 and section 6.4.3 how the integration of fast handover and HMIPv6 works.

4. Integration of security, mobility management and QoS, making use of the enhanced node concept, based on the proposed architectural framework

With the intelligence of enhanced node, the integration of security, mobility management and QoS becomes possible. The integration of security and mobility management can minimise the negative effect of security mechanism on the mobility protocols, in terms of introducing less handover latency or signalling overhead. The integration of security and QoS suggests here that important QoS messages can be secured, for instance, the QoS context transfer between neighbouring access routers/mobility agents to allow for smooth handover performance.

5. Specify the extensions to standard Mobile IP messages and propose new AAA commands

To enable proposed security solutions, extensions to Mobile IP messages and introduction of new AAA commands with defined set of Attribute-Value-Pairs (AVP) are required. In many of the
previous Mobile IP/AAA solutions, the details of message extension are not clarified. However, it is specified in each of the three solutions proposed in the thesis, the extension or modifications to Mobile IP messages. New AAA commands with defined AVPs are also specified, if the AAA messages are required.

6. Analytical model to simulate the signalling overhead of proposed security mechanisms

Some work has been carried out to evaluate the signalling overhead introduced by Mobile IP registration procedures, using analytical models. However, not much has been done to evaluate the signalling overhead introduced by security mechanisms. The analytical models have been used in the thesis to quantify the registration signalling cost of HMIPv6, FMIPv6 and the integration of them. Also, the signalling cost of proposed security mechanisms and some of the previous solutions are also evaluated. Thus, by comparison of signalling overhead, the advantage and disadvantage of the proposed security mechanism can be concluded.

Also, more accurate parameters are used in the analytical modelling. In previous work of evaluating signalling cost of registration messages in Mobile IP protocol and its variations using analytical models, the size of messages are not differentiated. For example, it is assumed that the size of binding update message is equal to that of binding acknowledgement message, in order to simplify the parameters in the model. However, more accurate parameters are used in my modelling process. I specify different message with its own size.

Publications are listed as follows,

6. “An Enhanced AAA Solution for Fast Handovers in HMIPv6 Networks” to be submitted to IET Communications.
2 Mobility Management and Security Mechanisms in Next Generation Mobile Networks

2.1 Mobility Management in Next Generation Mobile Networks

2.1.1 Ubiquitous Services over Next Generation Heterogeneous Network

A heterogeneous network is a network connecting computers and other end devices with different operating systems and protocols. In wireless networks, heterogeneous network is often referred to the network using several access technologies. For example, a wireless network which provides the internet service to an end user through a wireless Local Area Network (LAN) and maintains the connectivity when the user is switched to a GSM network. Ubiquitous access and services is one of the essential issues in the next generation heterogeneous networks. With the development of Bluetooth, WiFi, WiMax and Ultra-Wideband (UWB) access technologies, the dream of ubiquitous access has come closer to reality. That is why ubiquitous and pervasive services represent a major future revenue stream and meanwhile poses many practical challenges for service providers, telecommunication operators and pervasive technology manufacturers [1].

The barriers to delivery of ubiquitous services arise from the desire to deliver a wide mix of service to users with diverse device capabilities via multiple heterogeneous networks, as shown in Figure 2.1. When an end user wants to access data from a remote server using one or more network technologies, several issues arise from this scenario. For example, the nature of the data to be retrieved must be assessed (service/content perspective), the capabilities to deliver services with desired security and Quality-of-Service (QoS) level (network perspective) and the adaptation of the content/service to the user's pervasive environment (user perspective). In order to accelerate commercialisation of ubiquitous services, targeted innovations should be aimed at
removing the barriers to deployment and adoption from three perspectives – user, network and content/service providers.

The key barrier to accessing ubiquitous services from the network perspective arises from the need to manage delivery of multiple services within different security and QoS environments through multiple heterogeneous networks. It is therefore essential that different delivery networks should be empowered to operate in a cooperative manner. The presence of intelligence and interconnection among intelligent entities in such networks poses particular challenges. To address these challenges, an innovative network support sub-layer, which integrates security, mobility and QoS mechanisms, is proposed in [1]. Integration, in this context, incorporates both horizontal integration between the various service concepts that exist in the disparate networks, and vertical integration, where the support of security, mobility and QoS in the various participating networks is a key factor in end-to-end performance.

A network support sub-layer is defined in [1] to facilitate the co-operation among heterogeneous networks to support pervasive services, in a seamless, efficient and secured manner. The concept of network support sub-layer is proposed to integrate security, QoS and mobility management. The nodes with the network support sub-layer are referred to as enhanced nodes, which will be explained in detail in chapter 3. These networks are expected to use different security, mobility and QoS mechanisms. This makes co-operation among them a very complex technical issue. Since only a few enhanced nodes (enhanced nodes of each access networks) interact with each other, the proposed architecture will simplify the required functions and interaction mechanisms. There are two aspects for this approach. The first is to design a common network support sub-layer to integrate security, mobility and QoS functions efficiently. The second is to find out efficient mechanisms that enable the enhanced nodes with this common sub-layer in different access networks to interact with each other.
However, much research has recently been undertaken in proposing and designing security, mobility and QoS mechanisms based on the IP paradigm. In all of this work, different design approaches have been considered for each such mechanism in isolation, without considering their inherent interactions. When integrated into one network, they either do not work or, at least, do not work as well as expected. For example within the IST BRAIN [2] and MIND [3] projects, such mechanisms were designed and optimized separately but once put together, the overall performance was not as expected. The lesson learned from such research was to design them using the same approach and simultaneously with a common signalling protocol. Integration of security, mobility and QoS mechanisms within one network is necessary if efficient delivery of pervasive services is to become feasible for the network operator.

Security, mobility and QoS mechanisms are all beneficial in providing the features required to support their individual functions, but inevitably this leads to the network operation being pieced together in an ad-hoc manner, with no integration. Furthermore, there is no overall vision of how they can work together, to provide a single platform to enhance the network operations. Therefore it makes sense to adopt a common design approach for all these mechanisms using a common platform and, if possible, with one common signalling protocol for the network sub-layer.

The nodes with the sub-layer are referred to as enhanced nodes. It is located in a small number of nodes in the network, such as gateway, anchor point, etc. Within such a framework, translation of security, mobility and QoS will be required. A common representation of such mechanisms will be used in signalling between enhanced nodes to support this (horizontal integration). The enhanced nodes will operate within the constraints of their access networks, such as the ability to perform security related functionalities, to control routing and traffic flow, with the aim of meeting the desired end-to-end performance criteria (vertical integration). The use of such selected nodes in a heterogeneous network comprising security/mobility/QoS aware and unaware access networks potentially allows existing telecommunication networks to be enhanced, without the additional delays associated with network standardization, through selective upgrades of a limited number of network nodes.

The other part of this task is to come up with efficient mechanisms that enable the enhanced nodes with this common network sub-layer in different access networks to interact with each other. It is also essential to define a common inter-access signalling protocol for communication among the enhanced nodes in different access networks.

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment
to a wireless LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement [4].

### 2.1.2 Mobile IP Protocols

Mobile IP is an Internet Engineering Task Force (IETF) standard protocol that is designed to allow mobile end users to roam away from its home network while maintaining a permanent IP address. Thus, location independent routing of IP datagram is realized using Mobile IP. There are two versions of Mobile IP protocols: Mobile IPv4 [5] and Mobile IPv6 [4]. And several variations are introduced based on Mobile IP protocols, such as Hierarchical Mobile IPv6 (HMIPv6) [6], Fast handover for Mobile IPv6 (FMIPv6) [7] and Proxy Mobile IPv6 (PMIPv6) [8].

#### 2.1.2.1 Mobile IPv6

To allow the nodes to remain connected while moving in the IPv6 Internet, Mobile IPv6 (MIPv6) is proposed by IETF. The node can be always reached by its home address when it is in its home network. But packets destined to the node would not be able to reach it while the node is roaming away from its home network. Therefore, the mobility support for IPv6 node is needed to continue the communication no matter where the node is. MIPv6 allows an IPv6 node to move from one link to another with home address remaining the same. Packets destined to the node can be routed using its home address regardless of its current point of attachment. Therefore, continuous communication is achieved while the node is roaming in the visited network.

![Mobile IPv6 Domain](image)

Figure 2.2 Mobile IPv6 Domain

Figure 2.2 shows a typical Mobile IPv6 domain. When the Mobile Node (MN) moves from its home network to a foreign network, it obtains a new Care-of-Address (CoA), which provides information about the MN's current location. The MN then performs a Binding Update (BU) to its
Home Agent (HA), therefore the CoA is registered at HA. The HA creates a binding between the MN's home address and CoA and also sends a Binding Acknowledgement (BA) to MN. When the registration procedure is finished, the HA intercepts packets destined to the MN if a Correspondent Node (CN), whether mobile or stationary, wants to communicate with the MN. The HA then tunnels all packets from the CN to the MN using the MN's CoA. When the MN answers the CN, it may tunnel all its packets through the HA to the CN. Alternatively, it can use its current CoA to perform a BU to the CN and communicate with the CN directly after that. This process is called route optimization. Route optimization solves the problem of triangle routing, which is introduced by MIPv6's requirement to route packets destined for the MN through its home network. Route optimization is essential for the efficient operation of MIPv6, because it avoids congestion in the HA and also greatly reduces latency for communication and traffic load across the entire Internet [4].

MIPv6 has many same features with MIPv4, but it also provides many other improvements [4]. Some of the improvements are listed as follows,

- MIPv4 deploys special router “Foreign Agent (FA)” in the foreign network. While MIPv6 operates in the visited network without any particular support from special routers.
- MIPv6 supports route optimization, which greatly enhances the performance of Mobile IP routing. It is expected that route optimization can be applied on a global scale between any of the MN and the CN.
- In MIPv6, most packets destined to a MN while it is away from the home network are sent using an IPv6 routing header rather than IP encapsulation. It reduces the amount of overhead compared to MIPv4.

2.1.2.2 Hierarchical Mobile IPv6

In MIPv6, in order to maintain the connectivity between MN and CN, MN needs to sends BU to its HA and all of the CNs every time it changes point of attachment. The frequent location updates inevitably result in large handover disruption time and heavy network overhead. In order to eliminate the additional delays in the time-crucial handoff procedures and reduce the mobility signalling load on the external Internet, HMIPv6 is proposed to introduce extensions to IPv6 neighbour discovery and MIPv6 protocol. A local anchor point, called “Mobility Anchor Point (MAP)” is proposed in HMIPv6. MAP basically offers an anchor point for the MN to localize the mobility signalling, so that MIPv6 is beneficial from reduced network overhead with external networks.
MAP can be placed at any level in a hierarchical network. It provides localized mobility management by limiting the amount of mobility signalling out of its local domain in the following ways,

- MN sends a BU message to MAP rather than HA and CNs, when it enters a MAP domain. Since Global location update to HA is always a time-consuming procedure, with HA located far away from the visited network, the mobility signalling in HMIPv6 are considerably reduced.

- In MIPv6, MN sends BU to its HA and all of the CNs when it moves from one link to another, to maintain the connection. While, MN only needs to send one BU to its current MAP before the packets can be re-routed from its HA and the CNs. MAP is technically the local HA to the MN.

MAP not only help to improve the handover rate, but also can reduce the amount of signalling related to mobility. The goal in a domain oriented mobility management schemes like HMIPv6 is to limit the signalling messages locally within the region. That is due to the fact that BU are sent from MN directly to MAP rather than HA, meaning that MN’s exact position is hidden from the upper layer nodes. Thus the signalling messages in macro level get reduced as long as the MN stays in a specific region. In such a structure the MN has two CoAs: LCoA and RCoA. The MN registers the obtained address from its serving AR with its current MAP. This address is called “On-Link CoA” (LCoA), also referred to as local CoA. The MAP binds the LCoA with its own address which is called “Regional CoA” (RCoA). The source address of outgoing packets from the MN to the outer domain carries the MAP’s address. Therefore, the peer nodes just deal with the MAP and the incoming packets are addressed to the MAP as well. Then, MAP distributes the packets among the visiting MNs of its domain, according to its binding table [9].

Figure 2.3 shows a typical HMIPv6 domain and gives an example of the use of MAP in a foreign network. As illustrated in Figure 2.3, there are two MAPs covering the network domain and each of the MAP domains consists of several ARs. MAP can provide seamless handover as MN moves from AR1 to AR2. Upon arrival in a foreign network, MN discovers the global address of the serving MAP (RCoA). The address is stored in all of ARs in the MAP domain, and MN can be notified through router advertisement (RA) message. The process of discovering serving MAP and its related information is called “MAP discovery”. The MAP discovery also takes place as MN moves from MAP1 domain to MAP2 domain to notify the MN the change of serving MAP. The RA can be used to detect movement and inform the MN whether it has changed the MAP domain, through a MAP option. If the MN is still within the same MAP domain, it will receive the same MAP option in RA from the AR. If the MN moves across MAP domains, the
advertised MAP address would change. And upon detecting the change in MAP option, MN performs BU to the new MAP. The MN first registers with new MAP by sending it a BU containing its home address and LCoA. The home address used in the BU is the RCoA of MAP. The serving MAP stores the information in its binding cache and forwards packets received from HA or CNs to MN according to the information in the binding cache.

![Hierarchical Mobile IPv6 Domain](image)

**Figure 2.3 Hierarchical Mobile IPv6 Domain**

### 2.1.2.3 Fast Handover for Mobile IPv6

During a handover in MIPv6, there is a period when MN can not either receive or send any packets from its HA or CNs because of the protocol operations. The handover disruption time usually results from the MIPv6 operations, such as new CoA configuration, BU, especially the global BU to HA which is always far away from MN's current location. For the time-sensitive data, such as voice over IP (VoIP) service, large handover latency is not tolerable and it is essential that the MN can continuously send and receive packets while performing location updates. Therefore, FMIPv6 is proposed to reduce the handover latency. It enables the MN to send packets as soon as it detects a new subnet link and to receive packets as soon as its attachment to a new AR.

Figure 2.4 FMIPv6 Scenario

Figure 2.4 shows a simple scenario for FMIPv6. The MN is moving from the previous AR (PAR) to the new AR (NAR). In FMIPv6, even though a MN moves into a new domain, before it registers its New CoA (NCoA) to the HA/CN, packets sent from the HA/CN are delivered to the PAR first. Then they are tunnelled to the NAR by the PAR and finally arrive at the MN. Once the MN completes the registration of its NCoA to the HA/CN, packets will arrive at the MN directly via the NAR [10].

It is defined in [7] two types of fast handover, namely predictive fast handover and reactive fast handover. And there are also two kind of handover mode: MN initiated handover and network initiated handover. The basic operations of the MN initiated fast handover in predictive mode are shown in Figure 2.5 and can be explained as follows [7].

In a MN initiated handover, the MN sends an Router Solicitation for Proxy Advertisement (RtSolPr) to its previous AR (PAR) requesting information for a potential handover. PAR sends a
Proxy Router Advertisement (PrRtAdv) message as response. PrRtAdv contains information of the NAR, which includes AR's L2 address, AR's IP address and subnet prefix.

With AR information provided in the PrRtAdv message, the MN obtains a prospective New CoA (NCoA) which is the CoA valid on the New AR (NAR)'s subnet and sends an Fast BU (FBU) message to the PAR. FBU basically instructs PAR to tunnel packet towards NAR by binding Previous CoA (PCoA) to NCoA. Sending FBU message via PAR's link is recommended, however, FBU is sent via the NAR's link in reactive fast handover mode. In reactive mode, it is therefore essential that the NCoA used in FBU does not conflict with an address already in use by other MN on the same link.

Before sending a Fast BA (FBA) message to the MN as a response, PAR exchanges Handover Initiation (HI) and Handover Acknowledgement (HAck) messages with NAR. The exchange of HI and HAck messages is to determine whether the NCoA is valid. If NCoA is already in use in NAR's link, the NCoA is not valid and NAR will propose another NCoA, which will be transmitted to PAR in the HAck message.

PAR sends the FBA message to MN in response to FBU. The MN will be notified of the NCoA in FBA message, if there is a NCoA assigned by the NAR. And MN must use the assigned NCoA upon its attachment to the NAR.

In predictive mode, FBA is transmitted via the PAR's link, therefore, the packet tunnelling between PAR and NAR is possibly already in progress when MN handovers to the NAR. Upon MN's attachment to the NAR, MN sends a Fast Neighbour Advertisement (FNA) to the NAR immediately to announce the attachment, and to confirm the use of NCoA when the MN has not received a FBA message. Thus, the NAR can forward previously buffered and arriving packets to MN right away.

The difference between predictive fast handover and reactive fast handover is whether an FBU message is sent through PAR's link or not. The case in which the MN sends an FBU from NAR's link is reactive fast handover. The reactive handover also includes the scenario in which an FBU has been sent from PAR's link but an FBA has not been received before MN attaches to the NAR.

The handover can also be initiated by the network. In a network initiated handover, PAR sends an unsolicited PrRtAdv message containing the information of the NAR when the handover is about to be performed. The unsolicited PrRtAdv allows the network to inform the MN about geographically adjacent ARs without the MN's attempt to request the information. Upon receiving unsolicited PrRtAdv message, the MN configures a NCoA to be used in NAR's link, and sends a FBU message to PAR. Before receiving the FBU from MN, the PAR continues to

deliver packets to the MN via the PAR’s link. The network initiated handover can be used in some wireless technologies, as the handover control might reside in the network [7].

2.1.2.4 Integration of HMIPv6 and FMIPv6

Handover within One MAP Domain

HMIPv6 and FMIPv6 can be integrated to further enhance the fast handover and reduce the signalling overhead. It is proposed in [6] and [10] the mechanism to integrate HMIPv6 with FMIPv6 for mobility within one MAP domain.

The functionality of FMIPv6 procedure remains the same, although, the anchor point is moved from the PAR to MAP. Therefore, HI/HAck exchanges occur between the MAP and NAR in order to check the validity of NCoA. If NAR confirms that the NCoA is valid, a temporary tunnel is established.

The predictive mode of fast handover is considered. Upon receiving PrRtAdv message from PAR, MN discovers whether it is still in the same MAP domain by checking MAP address in the MAP address option. If the MAP address is the same as the address MN previously registers to, MN assumes that it is moving within one MAP domain. Therefore, the MN constructs NCoA using the NAR’s information, which is obtained from PrRtAdv message. The MN then sends FBU message to PAR, and the PAR forwards it to MAP. Having received FBU message, the MAP starts HI/HAck message exchanges with the NAR. Once HI/HAck exchanges are done, MAP assumes that the fast handover procedure is completed. Therefore, MAP sends a flush message [10] to the PAR to inform that its binding cache is about to be updated with NCoA. The MAP also sends the FBA message to NAR after the binding cache is updated. By then, MAP tunnels all the packets to MN using NCoA through NAR link. Having received the flush message from the MAP, the PAR starts to tunnel buffered packets by encapsulating the packets with NCoA as the destination address. When MN moves to NAR, it sends a FNA message to the NAR, asking the NAR to send packets. Packets arriving at the MN can be classified into two types: the packets sent along MAP \(\rightarrow\) PAR \(\rightarrow\) NAR path with PCoA as the destination address and the packets sent along MAP \(\rightarrow\) NAR path with NCoA as the destination address.

Handover between MAP Domains

During the handover process between MAPs the location update needs to be sent to the CN and the HA. The global location update is time-consuming, as home network and CNs could be far away from the visited network. In order to minimise the handover disruption time, fast handover needs to be implemented. During the handoff, the RCoA obtained from the mobility
agent changes and the packets that the CN transmits to the MN need to be re-addressed to the new RCoA of the new MAP. The handover happens between MAPs as shown in Figure 2.6 [11].

![Figure 2.6 Fast Handover between MAPs Scenario [11]](image_url)

During the handover period the packets arriving at Previous MAP (PMAP) are stored and buffered packets are redirected to New MAP (NMAP) after the fast handover registration is completed. This procedure is clearly illustrated in Figure 2.6. The MN associates itself with NMAP and obtains a new RCoA. In turn the MN then performs a global location update to its HA and CNs, which could result in large delays and packet loss. With fast handover enabled, packets generated by CNs will still be arriving at the MN’s old location (PMAP) during this handover period. To minimise the loss in packets, the PMAP redirects the packets it receives from the CN to the new location of the MN (NMAP). In turn NMAP tunnels these packets to the MN. The packets finally arrive at the new LCoA associated with the NAR that is geographically adjacent to PAR on the boundary of the PMAP domain. This will allow for a smooth inter-MAP handover as it allows the MN to continue to receive packets while updating its HA and, potentially, CN. To make the fast handover possible, the new location of the MN (address of NMAP) needs to be temporarily registered with the PMAP, also the PMAP needs be configured to forward packets to the NMAP. This can be done by the fast handover registration. Therefore the maximum delay experienced is the time it notify its PMAP about its new location. This delay can be minimised if the MAPs have prior knowledge of the surrounding MAPs as well as location information of the MN. Fast handover minimise the delays even further and provide stable QoS during handovers [11].
Figure 2.7 shows the signalling involved in inter-MAP domains fast handover. Depending on whether a FBA message is received or not on the PMAP's link, there are two modes of operations, namely the predictive mode and the reactive mode. Predictive mode is considered here. After the information for a potential handover is exchanged between MN and PAR through RtSolPr and PrRtAdv messages, the handover is triggered. The MN obtains the address of NMAP from MAP address option in PrRtAdv message and it also constructs the new LCoA to be used in the NAR's link. Then the MN initiates a FBU to the PMAP, instructing it to buffer the packets to MN with previous LCoA as the destination address. The PMAP and NMAP also exchange information through HI/HAck messages to negotiate with each other regarding the MN's handover. This includes validating the new LCoA that MN has constructed, with the help of NAR. Having received HAck message from NMAP, the PMAP sends a FBA message to MN and NMAP as the response to FBU. The fast handover registration is completed by now. Afterwards, the packets addressed to MN's previous location can be tunnelled from the PMAP to the NMAP. After the global location update finishes, the packets from CNs can be delivered to MN through NMAP's link as defined in HMIPv6 specification.

![Diagram of Fast Handover between MAPs](image)

**Figure 2.7 Signalling for Fast Handover between MAPs [12]**

Figure 2.8 gives an overview scenario of HMIPv6/FMIPv6 integration. It is clearly illustrated in the figure the packet redirection for fast handover with one MAP domain and between neighbouring MAPs.
Context transfer is performed between neighbouring ARs or neighbouring MAPs sometimes, such as the QoS context transfer between subnets to allow for stable QoS during and after handovers. Context transfer is being worked on in the IETF “Seamoby” working group [13].

2.1.3 Other Micro-mobility Protocols

Apart from HMIPv6, there are other existing IP micro-mobility protocols. Cellular IP and HAWAII are two examples.

Cellular IP was proposed by Columbia University and Ericsson in [14]. It allows routing IP datagrams to mobile host, and also provides support for local mobility, handoff and paging technique. Location management and handoff support are integrated with routing in Cellular IP networks. To minimise the control signalling, regular data packets transmitted by the mobile hosts are also used to refresh location information of the host. Cellular IP is intended to be used on the local level, such as in a campus or the metropolitan area network (MAN). It can also interwork with Mobile IP to provide support for wide area mobility, which is mobility between local cellular IP networks.

HAWAII was proposed by Lucent Bell Labs in [15]. HAWAII is a domain-based protocol for supporting mobility. Unlike Cellular IP, HAWAII does not replace IP but work above IP. Each station within the HAWAII network must not only act as an IP router but also support specific mobility functions. It uses path setup schemes which install host-based forwarding entries in particular routers to support intra-domain mobility. And it also interworks with mobile IP to
provide inter-domain macro-mobility. The path setup schemes reduce mobility related disruption and also reduce the mobility related updates by operating locally. In HAWAII, mobile host can retain the network address while moving within one domain, which simplifies the QoS support.

A comparison of MIPv6, HMIPv6, Cellular IP and HAWAII is provided in Table 2.1.

<table>
<thead>
<tr>
<th></th>
<th>MIPv6</th>
<th>HMIPv6</th>
<th>HAWAII</th>
<th>Cellular IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Connectivity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AAA and security</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Stable point of attachment</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Real-time traffic management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>QoS support</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dynamic address allocation</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Protocol layers</td>
<td>L3</td>
<td>L3</td>
<td>L3</td>
<td>L3</td>
</tr>
<tr>
<td>Paging support</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Location Update</td>
<td>Datagram tunneling</td>
<td>Update message</td>
<td>Update message</td>
<td>Data packet</td>
</tr>
<tr>
<td>Route optimization</td>
<td>Mobility binding</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mobility management</td>
<td>Global</td>
<td>Micro/global</td>
<td>Macro/global</td>
<td>Micro/Macro</td>
</tr>
<tr>
<td>Handoff control</td>
<td>Soft based</td>
<td>Soft anticipated handoff</td>
<td>Path setup schemes</td>
<td>Hard and soft</td>
</tr>
<tr>
<td>Signalling overhead</td>
<td>High</td>
<td>Micro: low Global: high</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Latency</td>
<td>High</td>
<td>Micro: low Global: high</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 2.1 Comparison of Mobile IP and other micro-mobility protocols [16]
2.2 Security Mechanisms for Mobile IP Networks

2.2.1 Security Techniques

The basic concepts of security techniques are introduced in the following section.

2.2.1.1 Concepts of Encryption/Decryption and algorithms

In cryptography, encryption means the process of transforming information (often referred to as plaintext) into encrypted information (referred to as ciphertext), using a key. Decryption is the reverse process, transforming ciphertext into plaintext. A cryptographic key is a parameter used in conjunction with a cryptographic algorithm to perform the encryption/decryption process. Some of the key management terminologies used in the thesis are explained below,

- Keying material: the information required to establish keys or trust relationship. In most cases, it refers to the data needed to derive the key rather than the key itself.
- Master key: the key used to derive other keying material or key. It might potentially be a symmetric key.
- Nonce: a non-repeating value, such as a pseudorandom number, which is used only once for a particular purpose, such as key derivation, anti-replay protection, etc.
- Key encrypting key (KEK): a key that is used for encryption/decryption of other keys. Key encryption is used to protect the key during transmission or storage. The key used in encryption is called KEK, and the key being encrypted is called the encrypted key. KEK is usually used in symmetric key encryption method [17].

The cryptographic algorithm is classified by National Institute of Standards and Technology (NIST) document [18] as follows:

- Hash algorithm: A cryptographic hash function is a procedure that takes an arbitrary block of data and returns a fixed-size cryptographic hash value. Any change to the input data would result in different hash value. There are two most widely adopted hash functions: SHA-1 which has an output size of 160 bits and MD5 which has an output size of 128 bits.
- Symmetric key algorithm: Symmetric key algorithm uses a single key to encrypt/decrypt data, and the key is a secret only shared between two network entities. Thus, symmetric keys are used as pairwise keys between two entities involved. For encryption purpose, there are two types of algorithms commonly used: American Encryption Standard (AES) and Triple Data Encryption Standard (3DES). A standard DES encryption key is 56 bits long. DES encryption is no longer considered strong enough for high security applications, as a distributed
computing project managed to crack a DES key in 22 hours and 15 minutes. It believed to be practically secure in the form of 3DES, which applies DES cipher algorithm three times. As DES's successor, AES keys can be 128, 192 or 256 bits long. Most commonly the 128 bit key length is used.

- Asymmetric key algorithm: Asymmetric key algorithm is also referred to as public key algorithms. In public key cryptography, two parties have two keys each: a private key that only the owner has, and a public key that is distributed to the other party. Encryption is usually done with the receiver's public key, so that only the receiver can decrypt the message using its private key. RSA (which stands for Rivest, Shamir and Adleman who defined it) is a widely used algorithm for public key cryptography.

2.2.1.2 Security Association

In Internet Protocol Security (IPSec) [19], SA is strictly defined in [20]. IPSec SA is a data structure that includes a specified set of information as well as the implementation details, such as what mode to use. To establish IPSec SA means that two network entities have agreed to use IPSec to secure the communication between them, and also agreed on more details, such as what protocol to use (Authentication Header (AH) protocol and/or Encapsulating security payload (ESP) protocol), what cryptographic transform to use, etc [17].

However, the term “security association” (SA) has been used in many other contexts. In a loose definition, it is the establishment of shared security information between two network entities to secure communication between them. It is a group of security parameters, such as cryptographic keys, lifetime of these keys, etc., to provide secure connection. Compared to the strict definition in IPSec protocol suite, the use of SA in other application could cause confusions. Therefore, the term “trust relationship” is used in this thesis instead.

2.2.1.3 Message Authentication Code (MAC)

In cryptography, a message authentication code (MAC) is a short piece of information which is used to authenticate a message. A MAC algorithm, also referred to as a keyed hash function, takes a secret key and a message to be authenticated as input, and produces a MAC value as output. The MAC value protects the message's integrity and authenticity, by allowing the receiver to verify any changes to the message content using the same secret key.

A framework, called HMAC (hash-based MAC) [21], was developed by IETF. It is a specific mechanism for calculating a MAC involving a cryptographic hash function and a secret key. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of
HMAC, and the MAC algorithm is termed as HMAC-MD5 or HMAC-SHA1 accordingly. HMAC calculation can be explained as [17],

\[ \text{HMAC} = H(K \oplus \text{outer pad}, H(K \oplus \text{inner pad}, \text{Message})) \]

where, H is the hash algorithm used; Key is the secret key shared between the sender and receiver of the message; Outer pad and inner pad are the padding applied to the original message, and they are constant values which have the same length as input data.

The sender of a message simply appends HMAC value to the message as,

\[ \text{Message, HMAC(Key, Message)} \]

and sends it to the receiver. HMAC-MD5 and HMAC-SHA1 produce an output value of length 16 bytes and 20 bytes respectively. It is recommended in HMAC specification that the length of key used to calculate HMAC should be at least as long as the output value of the hash function, in order to maintain the strength for the HMAC procedure.

HMAC can also provide anti-replay protection by adding a nonce in the calculation,

\[ \text{HMAC(Key, Message, Nonce)} \]

A replay attack means an adversary trying to record a message and replay it at a later stage. The nonce is a value that is used only once and it ensures the receiver that the message is not a replayed version of previous message.

### 2.2.2 Authentication, Authorization and Accounting (AAA) Architecture and Protocols

AAA, which is defined in [22], refers to Authentication, Authorization, and Accounting.

Authentication, in general, is the process of verifying an identity claimed by or for a system entity. An authentication process consists of two steps: identification step which is to present an identifier to the security system and verification step which is to generate authentication result that corroborates the binding between the entity and the identifier. Much work has been done in authentication for Mobile IP [23] [24]. Authentication in AAA solution basically involves validating the end users' identity prior to granting them network access. This process relies on the fact that the end user possesses a unique piece of information, such as a username/password combination, a secret key shared with the network, biometric data (like fingerprints) that serves as identification credentials, etc. The AAA server compares the authentication data presented by the
user with the data stored in its database. If the credentials match, the user is granted network access [25].

Authorization is the procedure of checking whether a system entity has the right or permission to access a particular system resource. To authorize means to grant such a right or permission. Authorization in AAA solution defines what rights and services the end user is allowed once network access is granted. It might include providing an IP address, making decision on which applications are available to the user, and so on. Authentication and authorization are usually performed together in an AAA enabled environment [25].

Accounting (the third "A") provides the methodology for collecting information about the end user’s resource consumption, which can then be used for the purpose of billing, auditing, and capacity planning [25].

The fundamental components of an AAA solution are illustrated in Figure 2.9. The AAA server is attached to the network and acts as a central repository for storing and distributing AAA related information. There might be multiple servers located in different domains of the network, and the servers can communicate with each other through AAA protocol. The network access server (NAS) is an entity that acts as the point of entry into the network. It can be a router, a terminal server, etc. AAA solution can be summarized in the following steps [25]:

- End user connects to NAS requesting access to the network.
- NAS, as an AAA client, collects and forwards the end user’s credentials to the AAA server through the network.
- AAA server processes the credentials and returns either an accept or reject response, and other relevant data to the AAA client.
- NAS notifies the end user whether access is granted or not for the specified resources.

![Figure 2.9 Fundamental Components of AAA Architecture](image)
The most widely used AAA protocols are Remote Authentication Dial-In User Service (RADIUS) and DIAMETER, which interestingly is not an acronym. They are introduced in following sections respectively.

### 2.2.2.1 RADIUS protocol

RADIUS is a well-known and widely deployed AAA protocol, which is the acronym for Remote Access Dial-In User Service. It was proposed in 1990s by Lucent to provide authentication and accounting services to the NAS devices. RADIUS working group was set up by IETF in 1996 to standardize the protocol's basic functions and message formats in [26] to provide authentication and authorization. The AAA working group in IETF also developed some successor protocols for improvements that better address other issues that are not covered in [26]. It was defined in [27] the use of RADIUS to deliver accounting information. Improvements are made in [28], [29] and [30] for additional extensions.

Some of the key features of RADIUS protocol are summarized below [28],

- **Attribute/value pairs (AVP).** RADIUS protocol carries AAA information encoded in variable length “Attribute-Length-Value” 3-tuples, which are called attributes or AVPs. New attribute values can be added without disturbing existing implementations of the protocol. Common examples of attributes include User-Name, User-Password, Framed-IP-Address (IP address for end user), and so on. A list of attributes supported by RADIUS is specified in [28].

- **Flexible authentication methods.** RADIUS can support multiple authentication mechanisms to authenticate the end user, such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

- **Client/server based operation model.** A RADIUS client resides on the NAS and communicates with a RADIUS server. The client requests and the server processes and responses. Additionally, a RADIUS server may serve as a proxy client for another RADIUS or authentication server.

- **Network security.** All communications between a RADIUS client and server are authenticated using a shared secret key which is never sent over the network. In addition, if user password is contained in RADIUS message, it is encrypted to prevent hackers from gaining it by snooping the network.

### 2.2.2.2 DIAMETER protocol

RADIUS was originally designed for small network devices supporting just a few end-users requiring simple server-based authentication. With the development of network access
technologies, it is necessary to provide AAA services for hundreds and thousands of concurrent end users accessing network services using a variety of technologies. This is beginning to place a burden on the functional capabilities of the existing AAA protocols. RADIUS also reserved some extensibility for new demands that can be anticipated. It kept being modified and amended for a great number of new requirements. Thus, RADIUS is exhausted by thousands of patches and is struggling keeping up with the environment. So it is time for developing a new AAA protocol with new structure to replace the RADIUS. Therefore, the IETF made the effort to develop a next-generation AAA protocol: DIAMETER.

It is defined in [31] DIAMETER basic elements. DIAMETER is a lightweight, peer-based AAA protocol designed to offer a scalable foundation for introducing new policy and AAA services over existing PPP and emerging (such as mobile IP) network technologies. It employs many of the RADIUS mechanisms, such as encoded AVPs, and proxy server support. DIAMETER also attempts to correct limitations inherent in the RADIUS protocol. Qualitative changes occur from RADIUS to DIAMETER. Some of the improvements are listed as follows,

- RADIUS attribute value cannot exceed 255 bytes, which may be too small in some applications, and a RADIUS component can only have 255 messages outstanding before an acknowledgment is required. For a NAS dealing with thousands of individual connections requiring AAA services, such limitations can result in disruption in services. While, Diameter supports a much larger attribute-value length and incorporates a reliable, window-based transport that permits a DIAMETER server to transmit as many messages as the NAS can handle.

- A RADIUS server cannot send unsolicited commands to a client. This makes it difficult to applications such as instructing the client to perform a specific accounting function, distributing useful information to the client, re-authentication on demand across heterogeneous deployment, etc. Support for server-initiated messages is mandatory in DIAMETER.

- DIAMETER also employs an improved retransmission and fail-over scheme that provides improved network resilience over the relatively primitive and slow technique used by RADIUS. DIAMETER fail-over mechanisms are defined in [32]. A pending queue for every peer is maintained at a DIAMETER element. Upon receiving a response message, the request is then removed from the queue [17].

- DIAMETER is backward compatible with RADIUS. Although DIAMETER does not share a common message format with RADIUS, efforts have been made to deploy the two protocols in the same network. The translation would need to happen through gateways to enable interaction between DIAMETER devices and legacy RADIUS devices.
2.2.2.3 Integration of AAA and Mobile IP

Needessity of AAA in Mobile IP

AAA protocols enhance Mobile IP application in the following aspects,

- Mobile IP protocols allow a MN to change its point of attachment to the Internet, although it does not provide any specific support for mobility across different administrative domains, which limits the application of Mobile IP in a large-scale deployment. AAA protocols, such as Diameter, enable MN to roam and obtain authenticated and authorized service in foreign domains [33].
- Mobile IP base specifications do not provide details about authentications and establishment of trust relationship between network elements, while AAA infrastructure brings the advantages of authentication and key management services.
- Mobile IP provides routing mechanisms for the MN's traffic as it roams across different networks, and AAA infrastructure makes sure that no business or trust agreements between the networks are violated and the security and integrity of the networks are not compromised as a result of the roaming [17].

Efforts have been made by researchers [34] and IETF Mobile IP working group/AAA working group to integrate MIP with AAA infrastructure. And the requirements of deploying AAA in Mobile IP networks are defined in [35]. DIAMETER extensions for MIPv4 [36] and DIAMETER support for MIPv6 [37], [38] have also been specified by IETF. This allows a MIPv4/MIPv6 node to receive continuous services from its service providers and also allows DIAMETER servers to authenticate, authorize and collect accounting information for the MIPv4/MIPv6 nodes.

AAA model in Mobile IP

![Figure 2.10 AAA Model in Mobile IP [33]](image-url)
Figure 2.10 illustrates a basic AAA model for Mobile IP application. There are two AAA servers located in home domain and visited domain, namely AAA server in Foreign domain (AAAF server) which provide local access to AAA infrastructure, and AAA server in Home domain (AAAH server) which is able to authenticate and authorize each of its clients.

When a client belonging to its home domain roams to a foreign domain, it requests local network resources. Before access to the resources is permitted, an attendant (such as AR) in the foreign domain asks the client to provide credentials that can be authenticated. The attendant forwards the request to AAASF server. These credentials may be something AAASF can understand, but in most cases they are assigned by, and understood only by AAASH. If AAASF server does not have enough information to carry out the verification for the credentials locally, it has to consult the external authority (the AAASH server), to verify the client's credentials. And once AAASH verifies the credentials, the local authority AAASF will notify the attendant about the successful negotiation. The attendant can then provide the requested resources to the client [33]. In many typical cases, the credentials are the information provided by a client to the AAA server in a message authentication code (MAC) constructed using a secret shared between the client and AAASH. The authorization depends only upon secure authentication of the credentials.

Modification to the basic model is required to support and utilize Local Security Associations (LSA). LSA was introduced by IETF in [39]. After a successful initial authentication of the mobile user through AAASH server, LSA allows the local domain (foreign network) to authenticate the user and perform key distribution without involvement of any external authority, such as AAASH server. Therefore, LSA optimizes AAA procedures in terms of reducing signalling load between network domains and delay caused by security signalling between network domains. There is no need for the requests to traverse the wide-area Internet that is likely to separate the AAASF and the AAASH, thus the latency introduced by security can be reduced. With LSA supported, AAA can easily provide services such as, user re-registration, user re-authentication, key distribution/refreshment, etc [33].

In order to allow MIPv4/v6 nodes to receive secured services from foreign domains, some of the applications need to be supported by DIAMETER. The DIAMETER Mobile IP application will allow:

- Local/remote network access control
- AAA server acts as a trusted third party allowing authentication of the mobile users and key distribution.
- LSA establishment between MN and the attendant

- Establishment of security association (SA) and distribution of keys or keying materials between entities (either MN, Mobile IP agents, or AAA entities)
- Secured transport of mobility signalling messages with the help of established SAs

The support for AAA in MIPv6 and MIPv4 is quite different when inter-domain deployment is considered. In MIPv4, FA can serve as an attendant to manage mobility and AAA functions on behalf of MN in foreign network. While MIPv6 does not have the equivalent of a FA and does not offer any mechanism by which the foreign network can authenticate and authorize the end user. HMIPv6 introduces MAP which is naturally an anchor point for mobility management functions, as well as access control and authentication of mobile users [40]. Thus, MAP would be an attendant providing the interface between client and foreign networks in the AAA infrastructure.

2.2.2.4 IPSec Interaction with AAA Protocols

Introduction to IPSec

Internet Protocol Security (IPSec) provides layer-3 security. This means that all IP packets can be protected, irrespective of the upper layer protocol being carried in the packet payloads, and that no re-engineering of applications is required in order to take advantage of the security provided by IPSec. The security services offered by IPSec include access control, connectionless integrity, data origin authentication, detection and rejection of replays, confidentiality via encryption, and limited traffic flow confidentiality. These are all delivered using symmetric key techniques. The IPSec protocols also support automated key management, with key exchange protocols using both symmetric and asymmetric cryptographic techniques [41].

IPSec protocols can be deployed in two modes: tunnel mode and transport mode. In tunnel mode cryptographic protection is provided for entire IP packets. In essence, a whole packet plus security field is treated as the new payload of an outer IP packet, with its own header, called the outer header. The original (inner) IP packet is to be encapsulated within the outer IP packet. In tunnel mode, IPSec processing is typically performed at security gateways on behalf of endpoint hosts. The use of gateways means that hosts need not be IPSec-aware, but that security is provided from gateway-to-gateway rather than in an end-to-end fashion. By contrast, in transport mode, the header of the original packet itself is preserved, some security fields are inserted, and the payload together with some header fields undergo cryptographic processing. Transport mode is typically used when end-to-end security services are needed, and provides protection mostly for the packet payload [41].
There are two main IPSec protocols which specify the actual cryptographic processing applied to packets. They are Authentication Header (AH) protocol [42] and Encapsulating Security Payload (ESP) protocol [43]. AH provides integrity protection, data origin authentication and anti-replay services for packets through the application of MAC algorithms and the inclusion of sequence numbers in packets. ESP provides similar services to AH, although the coverage of integrity protection is more limited. In addition, ESP also provides confidentiality and traffic flow confidentiality services through symmetric key encryption and variable length padding of packets [41].

**IPSec Usage in DIAMETER Protocol**

All Diameter implementations must support IPSec ESP protocol in transport mode with encryption and authentication algorithms to provide per-packet authentication, integrity protection and confidentiality, and also must support the relay protection mechanisms of IPSec [31].

It is also recommended in [31] that Diameter implementations must support Internet Key Exchange (IKE) [44] for peer authentication, negotiation of security associations and key management. As an important member of IPSec protocol suite, IKE Protocol provides the method for SA negotiation and associated cryptographic parameter establishment. The latest version of IKE, named IKEv2, provides a flexible set of methods for authentication and establishment of keys and other parameters, supporting both asymmetric and symmetric cryptographic methods [41]. Diameter implementations must support peer authentication using a pre-shared key and may also support certificate-based authentication using digital signatures [31].
Chapter 3

3 Architectural Framework

3.1 Introduction to the Framework

Figure 3.1 illustrates the architectural framework which the work is based on. Two IP-based access networks with the similar infrastructure are presented. Within each of the networks, the MN is moving between ARs. The MN’s home network needs to be involved when home registration or authentication is performed. Also, more than one Enhanced Node (EN) is located within one access network and they communicate with each other through signalling, including signalling within one access network and between access networks. AAA infrastructure is deployed in the framework, with AAAH server located in MN’s home network and AAAF server located in each of the foreign network. The AAAF server, which is located close to the ENs to help delivering secured services to the MN. It is also assumed that one gateway (GW) is located in each access network as an interface with the external IP networks. The architecture assumes a loose coupling between the networks involved where the access networks are connected through the core IP network and any interaction between the access networks has to go through the core IP network [45].

The aim of this IP network is to deploy QoS, security and Mobility Management (MM) mechanisms in order to provide enhanced services to users. However these mechanisms have interactions with each other and the performance of one is affected by the working of the others. One of the major issues to be addressed is providing satisfactory security and QoS during handovers. Many mechanisms have been proposed to solve this issue and the EN can play a vital role in this scenario. Also, from security point of view, the EN assists in providing MN the authenticated and authorized access control when it moves across access networks with the help of AAA servers. Another major area is in routing and traffic flow within the access network. The traffic flow within an access network with HMIPv6 micro-mobility architecture would flow through MAPs in the network creating bottlenecks and high congestions. Hence regulating traffic flow and avoiding such bottlenecks are vital for efficient performance of the access network. The
ENs can greatly improve the performance of existing mechanisms and provide solutions to many of the cross issues [46].

3.2 Enhanced Node

In this section, the architecture of Enhanced Node (EN) and framework of the EN describing its components and functionalities are presented.

The concept of network support sub-layer, which integrates security, QoS and Mobility Management as shown in Figure 3.2, is proposed in [1]. The nodes with the network support sub-layer are referred to as ENs.

The network support sub-layer is located in a small number of ENs in a network. The EN can be an access router, gateway, anchor point (MAP in HMIPv6), etc. Such selected ENs can be used in the heterogeneous networks comprising security/QoS/MM aware and unaware access networks.
With a couple of network entities upgraded into ENs, integration of security, QoS and mobility management can be achieved.

The primary functionality of the EN is to gather security, QoS and mobility information from various parts of the access network and across heterogeneous networks and share this information when required by different entities. As a result this will enhance the performance of existing network mechanisms and assist the translation of mechanisms between heterogeneous networks.

The EN is constituted of four major components namely: Security, QoS, mobility management (MM), radio resource management (RRM) and signalling as shown in Figure 3.3. These components interact with each other and consider the cross issues rather than operating individually. This is illustrated in the figure through the double headed arrows between the components [46]. Each of the components will be explained in detail in the following sections.

### 3.2.1 Security Component

The security component of the EN plays a vital role in delivering the secured ubiquitous services either within one access network or across heterogeneous access networks. Figure 3.4 shows the interactions between the security entity of the EN and the other entities of the network. The dotted lines illustrate the security services provided through the EN. As a security entity, it connects to the AAA servers and the AR. It provides the mobile end users with the authenticated and authorized access control. And it can also help in the process of securing the MN’s handover/fast handover procedures.

Before a MN can be granted the network access, it should be authenticated and authorized. The access control scheme interacts with AAA infrastructure to provide the MN authenticated network access. The EN, connecting with both of the AR and the AAA servers, can interact with relevant
AAA entities to perform the AAA procedures on behalf of the MN. Before a MN performs handover between ARs, it needs to be authenticated for the handover and the handover signalings need to be secured using handover keys. In this case, the EN consults with the local AAA server for authentication and key generation/distribution. The EN can be in charge of the security services throughout the networks, in terms of performing authentication and key generation process by interacting with the AAA framework.

![Figure 3.4 Security functionalities of enhanced node [46]](image)

### 3.2.2 Mobility Management Component

The mobility component of the EN provides the ability to manage the functions relating to mobility management within access network and across access networks. Mobile IP protocol is used to provide the mobility management functions. This entity can function as the MAP of HMIPv6, but can also enhance the existing mobility management mechanisms. It does this by providing them with additional information required to take optimal decisions regarding mobility within and more specifically across access networks [45]. For example, choose the optimal location and number of ENs to be placed in one network. The mobility entity will interact with other entities involved in providing mobility to MN as shown in Figure 3.5.

![Figure 3.5 Mobility entity's interaction with other entities [45]](image)
3.2.3 QoS Component

The QoS component of the EN plays a vital role in terms of providing QoS throughout the network and across heterogeneous networks. This entity provides a virtual link between access networks to share information regarding resources and other QoS parameters. Per-flow based QoS architecture like IntServ with resource reservations can benefit with the additional knowledge of the network in providing optimal resource reservations and minimizing blocking probability. Reestablishing traffic flows after handover can also be enhanced by this entity. With the greater overview knowledge of the network, traffic flows can be optimally redirected to the new destination minimizing delays. This entity will also work closely with routing in the network identifying the paths with the required QoS. Traffic flow and congestion management also come under this entity. Figure 3.6 shows some of the possible interactions between the QoS entity of the EN and the other entities of the network. The dotted lines designate non-physical entities such as traffic shaping, congestion control, traffic flow management etc [45].

![Figure 3.6 QoS entity's interaction with other entities][45]

3.2.4 Radio Resource Management and Signalling Components

The RRM entity provides the framework for managing radio resources during handovers. A typical scenario is during the occurrence of a handover, in which the EN could help identify the access point (AP) with the necessary radio resources for the MN to connect. This would not be possible without having a higher level of intelligence within the network [45].

The signalling entity plays an important part. This entity enables the EN to gather information and share information through signalling each other and other entities. Integration of security, QoS and MM within one network using a common signalling approach is necessary if efficient delivery of pervasive services is to become feasible for the network operator [45].
3.3 Security Threats and Requirements

In this section, the general security threats arising from the architectural framework are described, followed by the corresponding security requirements. Threat analysis is important as it allow us to identify the appropriate security requirements, and to subsequently propose security solutions.

3.3.1 Security Threat Analysis

As defined in [47], network security threats are typically divided into passive and active threats, which are then subdivided into other types of threats. Passive threat is a threat in which an unauthorized party gains access to an asset, but does not modify its content, such as eavesdropping. While in an active threat, an adversary makes modifications to a message, data stream, or file. Active threats include masquerading, replay, message modification, and denial-of service (DoS) threats [25].

Based on the architectural framework presented in section 3.1, I am aiming to solve the following threats:

- Eavesdropping. The adversary may monitor transmissions for message content at the network level. For example, when a MN is communicating with a CN, an adversary could eavesdrop to the conversation and learn some useful data such as the MN’s address, even when the meaningful data are encrypted.

- Masquerading. The adversary may impersonate as an authorized user and thereby gain certain unauthorized privileges. This includes the Man-In-The-Middle (MITM) attack. For example, an adversary could impersonate as a legitimate MN to access the network and to perform handover.

- Message modification. The adversary may alter a legitimate message in an unauthorized manner by deleting, adding to, changing, or reordering it. For example, an adversary could modify the important signalling messages, such as binding update, handover key request message, etc, if they are not properly protected.

- Replay. The adversary may monitor transmissions (passive threat) and retransmit messages as a legitimate user. Therefore, if a malicious entity in the network captures these messages, it can retransmit them to request the services that only the legitimate user is allowed to use. For example, an adversary can replay an access request message that carries a token only the legitimate user has, and gain access to the network.

- Denial-of-Service (DoS). An entity fails to perform its proper function or acts in a way that prevents other entities from performing their functions. The adversary may prevent, or prohibit
the normal use of communication facilities. For example, an adversary could repeat the QoS-
conditionalised binding updates in a path to book out all the available resources so that the
path will run out of resources for any legitimate requests.

It should be noted that many of the threats mentioned above are related to each other. Therefore, the realisation of one threat may possibly lead to the realisation of one or more other
threats.

3.3.2 Security Requirements

Based on the security threats presented in section 3.3.1, a set of general and specific security
requirements are derived in this section.

3.3.2.1 General Security Requirements

The general security requirements are listed below,

- Network Access Control. Access control makes sure that the unauthorized users are denied
network access, while the legitimate users are granted the network access that they are
authorized to use. The MN needs to be authenticated and authorized before it can enter the
access network.

- Authentication/Authorization. Authentication is the process of verifying an identity claimed by
or for a system entity, and authorization is to grant the right to access certain resources. They
can be performed together within the AAA infrastructure. The MN needs to be authenticated
and authorized for the services it requests, such as the handover.

- Integrity. It is to ensure that data have not been changed, destroyed, or lost in an unauthorized
or accidental manner. MAC is usually used to protect the integrity of a particular message,
such as handover key request message to the server.

- Confidentiality. It is the property that information is not made available or disclosed to any
unauthorized individuals, entities, or processes. Confidentiality should be applied to any
important signalling messages. Encryption is a common method to assure the data
confidentiality.

- Anti-replay. Anti-replay is to prevent the replay attack by stopping an intercepted message to
be sent to the recipient multiple times by an adversary. A timestamp based anti-replay method
is widely adopted. The sender includes a best estimate of the time in its message, and receiver
only accepts messages for which the timestamp is within a reasonable tolerance. Thus,
recording and retransmitting an old message is not possible for an adversary.
- **Availability/Prevention of DoS.** Availability ensures that network resources/services, such as bandwidth, are always available. It can also prevent the adversary from disturbing or misusing the network services leading to a DoS attack. The MN needs to be authenticated before sending out the QoS-conditionalised binding update to make sure it is not an adversary trying to reserve the resources.

### 3.3.2.2 Specific Security Requirements

Apart from the general security requirements, some specific security requirements are also derived based on the framework.

- **Protection of the handover signalling.** It is required to secure signalling involved in the handover procedures, such as the binding updates. So that the adversary can not by any means gain or even modify useful information by listening to the handover conversation.

- **Support of efficient handovers.** It is necessary that the security mechanisms have minimal negative effect on the registration and handover procedures. Therefore, the integration of security and mobility management is required.

- **Integration of security and QoS.** It is required to secure important QoS signalling, such as QoS-conditionalised BU, and context transfer messages.
Chapter 4

4 An Enhanced Solution for the Authenticated and Authorized Access Control

4.1 Previous work

In order to allow roaming in foreign networks, MN needs to register with its home network and CNs by sending BUs to the HA and all of the CNs it communicates with. Even with the introduction of MAP, the global location update still occurs every time MN changes MAP domain, and of course when MN enters a new foreign network. One round-trip-time (RRT) is needed to update the HA and this can be done simultaneously while the MN is updating the CNs. Before a MN can be granted the network access, the visited network should perform a security check, such as Authentication, Authorization and Accounting (AAA) on the MN. Therefore, the MN should identify itself by interacting with the AAA server in its home network. This is called the AAA solution and it is a time consuming process.

The multiple round trip delays required for Mobile IP registration and AAA solution can disrupt active connections. Minimizing this additional delay in the time-critical handover period will significantly improve the performance of Mobile IP protocols. In order to speed up the roaming between different access networks, the registration and AAA solution must be improved. There are several publications in this area. It was proposed in [40] an AAA solution for authenticated access for IPv6 supported mobility based on HMIPv6. The authentication request message is piggybacked with the Mobile IP registration request message, thus, the RRT required for authentication and registration is reduced. However, it does not specify the AAA messages to transmit the authentication request in AAA infrastructure, and further research needs to be done on how the AAA infrastructure could be used to establish SAs between MN and subnets they are visiting. So that when MN performs handover between subnets within one access network, no signalling between the visited and home domain are needed for authentication purpose. It was
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

proposed in [48] the concept of shadow registration to reduce the AAA solution cost. Its variants were also proposed in [49] [50] [51] [52] for Mobile IP. The key idea of shadow registration is to establish an SA in the neighbouring ARs a priori anticipating a possible handoff when the MN registers to the given subnet. Thus, when a MN performs handover to a neighbouring subnet, the AAA solution is processed locally within that subnet without traversing the wide Internet to the MN’s AAASH server in the home network [53]. It was also proposed in [53] a dynamic shadow registration scheme which can be applied to HMIPv6 network. However, no work has yet specified how the SA is established between MN and the visited network using AAA infrastructure. Also, the shadow registration scheme is proposed for handoffs between different ARs or between different mobility agents (such as MAP) within one access network, obviously more work needs to be done to propose a faster AAA solution for handover across access networks.

In this section, it is proposed an enhanced AAA solution for inter access networks handover. It provides mobile users with authenticated and authorized access control, and also specifies the SA establishment for securing the future Mobile IP signalling. In order to minimise the negative effect of AAA solution on the handover procedure, the authentication request is performed in a handover preparation phase before the MN actually attaches to the new access network.

4.2 AAA Architecture and Trust Model

4.2.1 AAA Architecture and Functionalities

As illustrated in Figure 4.1, there are two AAA servers: the AAA server in Foreign network (AAASF) and the AAA server in Home network (AAASH). Ideally, the EN should act as AAA client. The AAA client can initiate the AAA request on behalf of the MN, and it also presents the MN’s credential to the AAA servers, who can use the information to make a decision. If the EN does not have the ability to function as AAA client, it at least should be able to initiate the authentication request message. The minimum required functionality of EN is conversion or at least encapsulation of Mobile IP messages into AAA messages, and vice versa.

In a HMIPv6 network, the EN, with the MAP functionality, can be utilized to perform access control on MNs and interact with AAA infrastructure. The AAASF server interacts with AAASH server in performing the AAA process to authenticate the MN. In order to eliminate the large signalling overhead and handover latency introduced by traversing the wide Internet between visited network and home network, it is desired that the AAASF server can have the MN’s security credentials which can be used to verify whether a MN is allowed the network access. In this way,
the AAAF server can speed up the authenticated handoff process. In order to further enhance the handover process, it is proposed in the shadow registration concept [53] another AAA server in the visited network, namely AAAL server. As illustrated in Figure 4.1, Local AAA server (AAAL server) is located in the AR domain. The AAAF could pass the MN’s security credentials to the AAAL servers. Therefore, with extension of the AAA hierarchy (shown in dotted line in Figure 4.1), the AAA solution can be localized within the AR, even without the need to go back to the AAAF server in the EN domain.

In the AAA/Mobile IP integrated application, the AAA infrastructure needs to provide the following functions,

- Authenticate/Authorize the MN to access the network
- Establish SAs which can be used to secure the relevant Mobile IP signalling in the future

And in order to provide these functions, the following issues need to be solved,

- Mobile IP protocol should be extended to be able to liaise with AAA servers for the task of authenticating the MN
- Mobile IP protocol should be able to request the AAA servers to generate the SAs and keys for MN and Mobile IP agents. And the SAs and keys are generated for the purpose of securing future Mobile IP signalling and other important signalling, such as QoS related messages.
- Mobile IP protocol should have relevant authentication extensions to carry authentication request and key generation request.
- AAA protocol, such as DIAMETER, should be able to interact with Mobile IP agents. And new AVPs need to be defined to carry Mobile IP related request in AAA infrastructure.
In the proposed AAA solution, one more AAA server is required and it is co-located with the enhanced node (AAAF server). The AAAL server is acting as the AAA server in the subnet, connecting to the ARs. Under the new AAA hierarchy, the MN's credentials can be distributed by the AAAH server to all of the AAA servers in the access networks, including the AAA servers of the enhanced nodes and the AAAL servers. Therefore, there is no need to traverse the AAAF server and the AAAH server every time when authentication and authorization are required. When the MN moves within one enhanced node domain, across the enhanced node domains, or even across the access networks, the handover latency can be reduced. Both of the micromobility and macromobility handoff performance can be greatly improved by the new AAA hierarchy.

4.2.2 Trust Model for AAA/Mobile IP Application

Trust relationship (SAs) needs to be established for Mobile IP based on relationships provided by the AAA infrastructure. A trust model depends on several factors, such as network topology, administration policy of the network that the MN is about to connect with, etc. It is explained, in this section, the trust model based on a generic HMIPv6 network topology. It is assumed that the MN is trying to connect to a foreign network that belongs to a different administrative domain from the domain the MN is currently connecting with, and obviously, the target foreign network is separated from the MN's home network.

![Figure 4.2 Trust model for AAA-HMIP integration](image)

It is illustrated in Figure 4.2 the trust model for AAA-HMIP integration. The trust model includes the network entities involved in the signalling and illustrates the trust relationships existing between these elements. The target foreign network is served by a local AAA server (AAAF server), while the MN's home network is served by an AAAH server. The concept of SA here, denotes the security context between two network elements which defines keys, algorithms
used to perform security functionality related to AAA-MIP procedures. As shown in Figure 4.2, there are three types of SAs involved in AAA-HMIP integration procedure: pre-shared SA, AAA SA and Mobility SA. They will be explained in the following sections.

4.2.2.1 Pre-shared Security Association

Pre-shared SA is the SA that provides security for the AAA procedures when AAA is integrated with MIP protocols. Pre-shared SAs must exist prior to Mobile IP registration. As shown in Figure 4.2 (solid arrow), they are shared between HA and AAAH server, AAAH server and AAAF server, AAAF server and EN. It is assumed that both of EN and HA have a pre-shared trust relationship with the AAA server in its domain. In other words, pre-shared SAs exist between EN and AAAF server (EN-AAAF SA), and between HA and AAAH server (HA-AAAH SA). The pre-shared SA also exists between AAAH server and AAAF server (AAAF-AAAH SA). It ensures that both of AAAH server and AAAF server can trust the integrity of the messages transmitted between them, and the keying materials can also be transmitted between the two entities in a secured manner. Since AAAH server and AAAF server are located in different domains, the existed SA between them implies that these two domains must have either a direct trust relationship or trust established through brokers.

4.2.2.2 AAA Security Association

AAA SA, as shown by solid arrow in Figure 4.2, is the pre-shared SA between the MN and its AAAH server. It can be regarded as a special piece of pre-shared SA, as it is especially important for the authenticated and authorized access control. Since the MN shares an SA with AAAH server, the AAAH server can verify the MN’s credentials for the purpose of authentication and authorization. The AAAH server can also help both of MN and mobility agents to obtain required trust relationships, which would be used in the future.

It is assumed that each MN subscribed to a network service provider is given an identity or a set of credentials that can be verified by the AAA server within the domain. The credentials are the information that can be used to perform security functions, such as authentication, key generation, etc. In the application of AAA-MIP integration, the MN’s credentials are usually referred to as a key or the keying materials that can be used to derive the key. This particular key shared between MN and AAAH server is the essential component of the AAA SA. And the key is assumed to be a symmetric key in MIP specifications. In the occasions that the credentials assigned to the MN is public key based certificates, a symmetric key needs to be derived from the certificate.
4.2.2.3 Mobility Security Association

It is defined in [54] the term of mobility security association, which refers to the SA that the MN establishes with mobility agents, such as MAP, HA, etc. Unlike the pre-shared SA, mobility SA does not exist prior to Mobile IP registration. After the mobility SAs are established, the MN and mobility agents can authenticate the mobile IP control signalling, such as registration request, registration reply, etc.

It is specified in [54] the derivation of mobility SAs making use of an AAA SA in Mobile IPv4. A mobility SA in the specification is a simple connection that can be used to authenticate MIPv4 control traffic between a MN and HA and/or between a MN and FA. This mobility SA is identified by the two endpoints. Take the mobility SA between a MN and its HA for example, it can be identified by attributes, such as a MN IP address, a HA IP address, and a security parameter index (SPI).

Similarly, mobility SAs are also required in the AAA-HMIPv6 integrated application. As shown in Figure 4.2 (dotted arrow), mobility SAs are also required between a MN and the mobility agents in HMIPv6, such as EN, which has the functionality of MAP, and HA. The main purpose of these mobility SAs is not to provide secured connections for large volumes of Mobile IP traffic between the MN and the corresponding mobility agents. These SAs are only applicable for the Mobile IP control signalling, such as authentication of Mobile IP registration request and response messages. Based on the fact that the control messages take place less frequently and only account for a small portion of data comparing to the IP traffic, the possibility of security attacks compromising these keys are considerably lower. Therefore, the use of hash functions and nonces in delivering keying materials to the MN is acceptable, although it might does not satisfy the cryptography fans. Please also be noted that IPSec protocols can be used to secure date packets.

4.3 Authenticated and authorized network access mechanism

The proposed authenticated and authorized network access mechanism provides the MN with the authenticated access control. And it also generates a handover key (Kaaa_en), which can be used to secure the signalling between the serving and target access networks. This key can be also used to secure the handover process in the target access work, as the security credentials can be distributed through the AAA hierarchy.

4.3.1 Assumptions

The following assumptions are made for the proposed mechanism:
- Overlapping of serving network and target networks

During the inter access networks handover from a serving network to a target network, it is assumed that the MN is in the coverage of both the networks, i.e. the two networks are overlapping sufficiently for the MN to prepare for the handover. The overlapping is necessary for the MN to receive signal from the target network before it loses coverage from the serving network. The required size of the overlap between the coverage of the two networks depends on the max speed of the MN [55].

- Trust relationship

It is also assumed that the required trust relationship has been established beforehand, as explained in section 4.2.2. As illustrated in Figure 4.3, the AAAH server shares secrets with the MN and AAA servers of the serving and target access networks respectively: Ks, K_aka1 and K_aka2. And the AAAF servers in the serving visited network and target visited network share secrets with the corresponding ENs respectively: K_en1 in the serving access network and K_en2 in the target access network.

![Figure 4.3 Pre-established trust relationship](image)

**4.3.2 Description of the Mechanism**

The mechanism is illustrated in Figure 4.4 and signalling is explained accordingly as follows:

1. The MN is about to perform handover from the serving network to the target network. It listens to a Router Advertisement (RA) message sent by the target AR in the target
network. The common Challenge/Response authentication method for MIPv4 defined in [56] is applied here. The target EN provides MN with a challenge on behalf of the HA through an extension to a RA [56]. The MN hashes the challenge with a pre-shared secret key with the home network (Ks), and creates a response as,

\[
\text{Response} = \text{HMAC SHA1}(Ks | \text{Challenge}),
\]

The MN then sends the challenge together with the hashed response over to the home network via the AAA infrastructure and waits for the response from the home domain. The information for the target EN, such as global IP address of the target EN, is also included in the RA message.

2. The MN initiates a Handover Preparation Request (Handover Prep Req.) message and forwards it to the serving AR. In this request message, the Network Access Identifier (NAI: MN ID@Realm) is included. Other information includes: handover key request extension and MN_AAA authentication request extension, which is the hashed response. The keying materials generated by the AAAH server after the access is granted will be distributed. The generated key Kaaa_en can be used in the new access network for the registration purpose. It can also be used to secure the signalling between the serving enhanced node and the target enhanced node if necessary, for example, QoS context transfer.

3. The serving AR forwards the Handover Preparation Request message to its serving EN.

4. Upon receiving the Handover Preparation Request message from an AR in its domain, the EN, as an AAA client, initiates an AAA request message, encapsulating the information in the Handover Prep Req. message. The AAA request message is sent to the AAAF server.

5. The AAAF server discovers that the AAA request cannot be resolved locally, and then forwards the AAA Req. message to the AAAH server according to “Realm” field in the NAI.

6. Upon receiving the AAA Req. message, the AAAH server should now authenticate the MN by comparing the “response” to the hashed result in its database. Depending on the authentication result, the AAAH server takes different actions.
   a. If the authentication is unsuccessful, the MN will be denied the network access and would be notified through the AAA response message to serving AAAF server.
   b. If the authentication is successful, the following steps are performed,
      i. The AAAH server generates the key Kaaa_en as follows,
      \[
      \text{Kaaa}_\text{en} = \text{HMAC SHA1}(Ks, \text{MN ID} | \text{N_aaa} | \text{EN1_ID} | \text{EN2_ID}),
      \]
where, N_ana is a nonce generated by the AAAH server, EN1_ID is the global IP address of the serving EN and EN2_ID is the global IP address of the target EN.

ii. The AAAH server sends the key/keying material to the serving AAAF servers in the AAA response message. There are two different ways to secure the key/keying material: encrypt the whole message with the pre-shared K_ana1 or encrypt the AVPs that carry the key/keying material with K_ana1. And in order to save the computational cost, the latter one is always preferred. Also, integrity can be provided by appending MAC to the whole message or just to the session key/keying materials AVP:

\[
\text{HMAC (K_ana1, K_ana1(K_ana_en)), K_ana1(K_ana_en),}
\]

Where, K_ana1 is the pre-shared secret between the AAAH server and the serving AAAF server. K_ana1 is used as a KEK to encrypt K_ana_en and related keying materials. It can be also used to calculate the MAC option of the message field.

iii. Upon receiving the AAA response message from the AAAH server, the serving AAAF server can validate MAC using K_ana1. After successful validation, the serving AAAF server decrypts K_ana_en using K_ana1.

7. The AAAH server sends an unsolicited AAA response messages to target AAAF server, informing the relevant key/keying material. The information can be secured in a similar way as described in 6-b-ii (AAAH server→serving AAAF server). If MAC option is needed to provide integrity, then

\[
\text{HMAC (K_ana2, K_ana2(K_ana_en)), K_ana2(K_ana_en);}\]

Where, K_ana2 is the pre-shared secret between the AAAH server and the target AAAF server. Upon receiving the AAA response message from the AAAH server, the target AAAF server validates MAC using K_ana2. After successful validation, the target AAAF server decrypts K_ana_en using K_ana2.

8. The target AAAF server sends an AAA response message to the target EN in the target foreign network. The information can be secured in a similar way as described in 6-b-ii (AAAH server→serving AAAF server). If MAC is included in this message for authentication and integrity purpose, then:

\[
\text{HMAC (K_en2, K_en2(K_ana_en)), K_en2(K_ana_en),}
\]

where, K_en2 is the pre-shared secret between the target AAAF server and the target EN.
Upon receiving the AAA response message from the target AAAF server, the target EN can validate MAC using K\_en2. After successful validation, the target EN decrypts Kaaa\_en using K\_en2.

9. The serving AAAF server forwards AAA response message to the serving EN. The AAA Resp. message includes the following information:
   a. the keying materials that the MN needs to generate Kaaa\_en: N\_aaa, MN ID, EN1\_ID, EN2\_ID and the key generation algorithm. The information can be secured using pre-shared key K\_en1.
   b. Kaaa\_en is transmitted either through an encrypted channel or in an encrypted AVP, using the pre-shared key between serving AAAF server and serving EN. If MAC is included in this message for integrity purpose, then:

   \[\text{HMAC (K\_en1, K\_en1(Kaaa\_en)), K\_en1(Kaaa\_en)}\]

   where, K\_en1 is the pre-shared secret between the serving AAAF server and the serving EN. Upon receiving the AAA response message from the serving AAAF server, the serving EN can validate MAC using K\_en1. After successful validation, the serving EN decrypts Kaaa\_en using K\_en1.
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

10. The EN, as an AAA client, converts the AAA Resp. message into a Handover preparation reply message as the response to the Handover Prep Req. message, and sends the Handover Prep Rep. message to the serving AR.

11. The serving AR sends the Handover Prep Rep. message to the MN. It includes the following information:
   a. NAI extension: MN ID@Realm;
   b. Handover key response extension: keying materials that MN needs to generate Kaaa_en;
   c. MN AAA authentication response extension: authentication result, indicating whether the network access is granted or not.

   After the MN receives the Handover Prep Rep. message, it generates Kaaa_en, using the keying materials obtained from the Handover Prep Rep. message and the pre-shared secret with the AAAH server (Ks).

4.3.3 Benefits of the Mechanism

Trust relationship is established among network entities, so that secured communication can be achieved making use of the existed trust as mentioned in section 4.3.1. The usage of Kaaa_en can be summarized in the following two ways:

1. Kaaa_en can be used to secure the communication between the serving EN and target EN in the neighbouring access networks. For instance, QoS context transfer may need to be performed between the serving and target ENs in different access networks. It is proposed in [55] a combined mobility and QoS framework for heterogeneous networks. More details are explained in Appendix A. In this framework, a combined mobility and QoS context transfer takes place between the ENs in different access networks. Therefore, it is essential that trust is established prior to MN’s handover to the new access network, so that the necessary context transfer can be secured.

2. Kaaa_en can be derived by the MN that has been granted the authenticated and authorized network access, using the keying materials obtained from the Handover Prep Rep. message. Thus, trust relationship is established between MN and target EN/target AAAF server. Kaaa_en can be used in the target access network to secure mobility signalling between the MN and the target EN, such as BU and BA. In the case where re-authentication of the MN is needed, there is no need to traverse the wide internet in order to reach the MN’s home domain, because the established trust between MN and the local AAA server (AAAF server in target access network). In another word, since AAAF server and the MN now shares a
secret, the authentication can be performed locally by the AAAF server without going back to the AAAH server in MN’s home network.

4.3.4 Compatibility with the localized AAA solution

The concept of shadow registration was explained in section 4.1 and the AAA hierarchy for shadow registration was described in section 4.2.1. The idea of shadow registration is to establish the local security association a priori anticipating a possible handoff when the MN registers to the given subnet, for instance, given AR. Thus, when a MN performs handover to a neighbouring subnet, the AAA solution is processed locally within the new subnet without traversing the wide Internet to the MN’s AAAH server in the home network. The process for shadow registration was defined and enhanced in [48], [49], [50], [51] and [52], and an improved solution, dynamic shadow registration, was proposed in [53]. However, none of those previous work investigated how the shadow registration is realized with regard to the establishment of local security association.

The proposed solution here can be extended to facilitate the localized AAA solution. In order to implement the extension, an enhanced AAA hierarchy needs to be employed, as illustrated in Figure 4.1. Apart from the AAAF server in the visited network, another local AAA server, namely AAAL server, is required in the AR domain. Thus, the AAA solution can be optimized, with AAAF passing the MN’s security credentials to the AAAL servers. The AAA solution can be localized within the AR, even without the need to go back to the AAAF server in the enhanced node domain. The extended AAA/HMIPv6 integrated architecture for shadow registration is shown in Figure 4.5.

In the HMIPv6 network, the enhanced node (MAP) can interact with the AAA infrastructure to perform authenticated access control on MNs. The AAAF server needs to consult with AAAH server in performing the AAA solution for a newly entered MN. An AAAF server in the enhanced node level can then store the MN’s security credentials after the MN is allowed network access. Thus, the AAAF server can speed up the authentication process by having the MN’s security credentials which can be used to verify the MN. As shown in Figure 4.5, during the handoff between ARs within one enhanced node domain, the AAAF server could pass the MN’s security credentials to the AAAL servers located in the AR’s domain to avoid performing the AAA process involving the AAAH server. Therefore, the AAA solution is localized even in the subnet (AR) domains. Figure 4.5 shows the network architecture for the localized AAA solution in HMIPv6 network.
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

Since the distribution of either actual key or keying materials needs to be done in a secured manner, SAs are necessary for distributing the MN's security credentials to the local AAA server (AAAL server) in the AR's domain. Except the pre-shared secrets illustrated in Figure 4.3, additional SAs are required between entities in the AAA architecture. As shown in Figure 4.6, SAs are needed between AAAF server and the AAAL servers in the enhanced node domain.

![Figure 4.5 Extended AAA/HMIPv6 integrated architecture](image)

![Figure 4.6 Additional SAs for the extended AAA architecture](image)

The secure distribution of keys or keying materials can be achieved in the following ways.
- Key wrapping method. If the two communication end points have trust relationship, the key wrapping method can be used for key distribution. It uses a symmetric key, which is shared by the two end parties, to encrypt the keys or keying materials. The symmetric key is also referred to as key encryption key (KEK). It is straightforward to use this key wrapping method for distributing MN's security credentials from the AAAF server to the AAAL servers, as AAAF server and AAAL server shares a secret (shown in Figure 4.6).

- Trusted third party. If the two communication end points have trust relationship, it is also popular to use a third party trusted by the two end points to perform the key distribution. For instance, AAA server could usually act as a trusted third party. As the key distribution is required from AAAF server to AAAL servers, it is not desired to involve another AAA server that can act as a trusted third party. For example, it is not natural to involve AAAH server again for key distribution between AAAF server and AAAL servers, because it is basically against the concept of localized AAA solution.

4.4 Syntax and Semantics of the Messages

4.4.1 Protocols Used between Different Network Entities

![Figure 4.7 Protocols between network entities](image)

In order to achieve the authenticated access control and to deliver the key/keying materials to the relevant networks entities, both of AAA protocol and mobile IP protocol should be involved. Figure 4.7 emphasizes the protocols to be used between different network entities. Mobile IP protocol is used between the MN and mobility agent, such as enhanced node. If the HA needs to be involved in some scenarios, the protocol between MN and HA is also Mobile IP. AAA protocol is used in the AAA infrastructure: between AAAH server and AAAF server, and
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

between AAAF server and enhanced node. As part of the AAA infrastructure, mobility agent, such as enhanced node, can function as an AAA client. Since requiring all of the AAA client’s functionality might become a burden for a mobility agent, it is acceptable to have only the essential functions. The minimal required functionalities are listed as follows,

- Interact with AAA server. The mobility agent should be able to convert or at least encapsulate message into a format that AAA server can understand (such as AAA request message) and vice versa.
- Have pre-shared SA with AAA server. Hence, the key can be delivered to the mobility agent through AAA protocol either over an encrypted channel or in the encrypted attributes.

It should be noted that DIAMETER should be used as the protocol for AAA infrastructure here, rather than RADIUS. This is not only due to the limitations imposed by AAA protocol such as RADIUS, but also the lack of integration of RADUIS and Mobile IP specifications. Compared to other AAA protocols, DIAMETER provides detailed specification for Mobile IP support, and most of them are standardized by IETF. On the contrary, very few IETF standards exist for RADIUS support of any Mobile IP protocols, however, there are some efforts by various communities (such as 3GPP2) designing their own specification for RADIUS/Mobile IP integration.

4.4.2 Extensions for Mobile IP Protocol

Extensions are needed for both of the Mobile IP protocol and DIAMETER protocol in order to support the proposed DIAMETER/MIP application. The extensions for Mobile IP protocols are possible because of the flexibility of mobility options. New mobility options can be defined to enable new applications. The syntax and semantics of the messages are explained in the following sections.

1. Handover Preparation Request message (MN → server AR → serving Enhanced Node)

It uses Mobile IP mobility header with a few new mobility options. The mobility options required are explained as follows,

a. HK request extension

MN needs to request a nonce from the AAAH server, which would be used by the MN as keying material to generate the key. When this extension is discovered, the mobility agent should interact with AAA servers to request key/keying materials. Table 4.1 describes the message fields of a generalized key generation nonce request extension, which is used here to request keying materials.
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the extension, in addition to those defined in the Mobile IP specification. Type number=40</td>
</tr>
<tr>
<td>Subtype</td>
<td>A number assigned to identify the way in which the Nonce Request Subtype Data is to be used when generating the registration key. When AAA is used, subtype number=1</td>
</tr>
<tr>
<td>Length</td>
<td>Length of the extension. It is equal to the number of bytes in the Subtype Data field plus 4 (for SPI)</td>
</tr>
<tr>
<td>MN SPI</td>
<td>SPI that the MN would assign for the SA created for use with the generated key. The relevant mobility agent (such as enhanced node) includes this SPI in the authentication extensions for messages from the mobility agent to the MN.</td>
</tr>
<tr>
<td>Key Generation Nonce Request Subtype Data</td>
<td>Data needed to carry out the generation of the key on behalf of the MN.</td>
</tr>
</tbody>
</table>

Table 4.1 Generalized key generation nonce request extension

b. MN-AAA Authentication extension

This mobility allows the MN to be authenticated by the AAA servers. It includes materials that AAAH server needs to authenticate the MN. A generalized Mobile IP authentication extension is introduced in [56], which allows the MN to be authenticated by a generic verification infrastructure. Table 4.2 illustrates the message format of the generalized Mobile IP authentication extension with the descriptions.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the extension, in addition to those defined in the Mobile IP specification. Type number=36</td>
</tr>
<tr>
<td>Subtype</td>
<td>A number assigned to identify the authentication strategy. For instance, when AAA server is used, it is assigned to be 1, and it is called “MN-AAA authentication extension”</td>
</tr>
<tr>
<td>Length</td>
<td>4 (for SPI) plus the number of octets in the authenticator field. It should be at least 20.</td>
</tr>
<tr>
<td>SPI</td>
<td>Security parameter index</td>
</tr>
<tr>
<td>Authenticator</td>
<td>The length is variable, subject to different authentication method. The MN uses the AAA key it shares with the AAAH server to calculate the authenticator field. It is a hashed message authentication code-MD5/SHA1 (HMAC-MD5 or HMAC-SHA1)</td>
</tr>
</tbody>
</table>

Table 4.2 Generalized authentication extension [56]

The challenge/response authentication mechanism is used in the proposed solution, hence, the authenticator is calculated as,

$$\text{Authenticator} = \text{HMAC-MD5/SHA1}(\text{challenge}, K_s)$$
It is noticed that both of MD5 [57] and SHA1 [58] can be used to compute the authenticator. Since SHA1 provides stronger security protect than MD5 in terms of hashed MAC, the use of HMAC-SHA1 is preferred.

The other mobility options included in the handover Prep. Request message include NAI extension and MN-FA challenge extension.

2. Handover Preparation Reply message (serving Enhanced Node \(\rightarrow\) server AR \(\rightarrow\) MN)

It uses Mobile IP mobility header with a few new mobility options. The mobility options required are explained as follows,

a. HK response extension

It carries the nonce from the AAAH server that MN needs to create the key. Table 4.3 describes the message fields of a generalized key generation nonce reply extension.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the extension, in addition to those defined in the Mobile IP</td>
</tr>
<tr>
<td></td>
<td>specification. Type number=41.</td>
</tr>
<tr>
<td>Subtype</td>
<td>A number assigned to identify the way in which the Nonce Reply Subtype</td>
</tr>
<tr>
<td></td>
<td>Data is to be used to obtain the key. Subtype number=1, if the nonce is from</td>
</tr>
<tr>
<td></td>
<td>AAA server.</td>
</tr>
<tr>
<td>Length</td>
<td>It is equal to the number of bytes in the Nonce Reply Subtype Data.</td>
</tr>
<tr>
<td>Key Generation Nonce</td>
<td>The nonce, along with any other keying materials needed by the MN to</td>
</tr>
<tr>
<td>Reply Subtype Data</td>
<td>derive the key.</td>
</tr>
</tbody>
</table>

Table 4.3 Generalized key generation nonce reply extension

b. MN AAA authentication response extension

A flag is used to indicate the authentication result. "Flag=1" indicates that network access is granted, while "Flag=0" suggests that network access is denied.

If integrity protection is needed for the handover preparation reply message, one more authentication extension, whose value is calculated using the generated key, can be inserted. By verifying this authentication extension, the MN can trust the handover preparation reply message.

The other mobility options included in the handover Prep. reply message include NAI extension and key lifetime extension.
4.4.3 Extensions for AAA Protocol

The AAA protocol (DIAMETER) need to interact with the relevant mobility agents. In terms of extensions required in AAA protocol to achieve the DIAMETER/MIP integration, it basically implies the following points:

- Support of the Mobile IP related authentication method and key generation at the AAA server needs to be defined.
- DIAMETER protocol needs to define the AVPs for carrying Mobile IP related information in the AAA infrastructure. And of course, the DIAMETER messages to carry the AVP need to be specified as well. AVPs usually carry specific authentication, authorization, accounting, routing and security information as well as configuration details for AAA exchanges. AAA protocols can support creation of new AVP for new applications.

In IETF’s AAA working group, the DIAMETER applications for MIPv4/v6 have been defined in [36] [38] and [37]. In these documents, DIAMETER Mobile IP application defines new commands and specific AVPs to transport Mobile IP related information in the AAA infrastructure. Some more functionalities are also introduced to assist the application. For example, DIAMETER makes use of the MN’s NAI to help the routing of DIAMETER messages to the AAAH server.

1. AAA Request message (serving EN -> serving AAAF server -> AAAH server)

DIAMETER defines a new command “AA-Mobile Node Request (AMR)” which can be used for interaction from mobility agent (such as EN) to DIAMETER server (either AAAF or AAAH server). Through AMR command, mobility agent can forward the MN’s authentication request, key generation request and other related information to the AAA servers, which can then make decisions and generate key/keying materials. See Appendix B for the complete message field for AMA command. Only a few essential fields are explained here.

a. User-Name AVP

AVP Code=1. The data field contains MN’s NAI.

b. MIP-Authenticator AVP

AVP Code=488. The data field contains the authenticator data from the received handover prep. request message. The mobility agent extracts this data from the MN-AAA Authentication extension included in the received handover prep. request message. It will be used by the AAAH server to verify the MN.

c. MIP-MN-AAA-Auth AVP
AVP Code=322. It is a grouped AVP, consisting of many sub-AVPs which include information to help the AAAH server to calculate the authenticator value. By comparing the value AAAH server calculated itself with the copy MN provides, the AAAH server is able to verify the MN.

d. MIP6-Feature-Vector AVP

AVP Code=124. It consists of many flags with values set by the mobility agent or local AAA servers. The flags indicate different information to the AAAH server. For example, flag=16 suggests that the MN requests the AAAH server to generate key/keying materials.

e. MIP-challenge AVP

A new AVP, similar to MIP-FA-Challenge AVP (AVP code=344). The data field contains the challenge that MN and AAAH use in the challenge-response mechanism.

2. AAA Response message (AAAH server → target AAAF server → target EN, AAAH server → serving AAAF server → serving EN)

DIAMETER defines a new command “AA-Mobile Node Answer (AMA)” which can be used for interaction from DIAMETER server (either AAAF or AAAH server) to mobility agent (such as EN) that sent the AMR command. In the AMA command, AAA server can deliver useful information to mobility agent through AVPs. The information includes authentication result, the keying materials that MN needs to derive the key, etc. See Appendix B for the complete message field for AMA command. Only a few essential fields are explained here.

a. Result-Code AVP

AVP code=268. The value can be either indicating success or failure. It is used to inform a peer whether a request has been successfully accepted or declined.

b. User-Name AVP

AVP Code=1. The data field contains MN’s NAI.

c. MIP-Session-Key AVP

AVP Code=343. The data field contains the session key generated by the AAAH server and sent to the mobility agent.

d. MIP-MN-to-MAP MSA AVP

A new AVP with AVP code to be assigned. It is similar to MIP-MN-to-FA-MSA AVP (AVP code=325). It is a grouped AVP carried in AMA message. It includes the information MN needs to generate the key, such as nonce, key generation algorithm type, etc.
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

e. MIP-MSA-Lifetime AVP

AVP Code=367. The data field contains the period of time for which the keys/keying materials are valid.

4.5 Analytical Models

Analytical models are used to evaluate the proposed solution. There are two aspects of the modelling: network model and user mobility model. The network model describes the network layout configuration, while the user mobility model is utilized to define the mobility pattern of the mobile terminals. Both of the two aspects will be explained in detail in this section.

4.5.1 Network Model

It is assumed here a two-dimensional (2-D) cellular configuration, the hexagonal network layout such as shown in Figure 4.8. It is also assumed that each domain managed by an enhanced node has the same number of rings of ARs. Each cell is surrounded by several rings of cells. The innermost cell 0 is called the centre cell; cells are labelled “1” form the first ring around cell “0” and so forth. Each ring is labelled according to its distance from the centre cell such that ring $r_1$ refers to the cells in the first ring away from the centre cell. In general, $r_k$ ($k=1, 2, \ldots$) refers to the $k^{th}$ ring away from the centre. Let $C(K)$ be a cluster of cells and the outmost cells are in the $k^{th}$ ring, e.g., $C(3)$ in of Figure 4.8 (1). The number of cells in $k^{th}$ ring is $6 \times k$. And the number of cells $N(K)$ in $C(K)$ is as follows,

$$N(K) = \sum_{k=1}^{K} 6 \times k + 1 = 3(K+1) \times K + 1$$

Eq. 4-1

where $K$ denotes the outmost ring, e.g., $K=3$ in Figure 4.8 (1).

Figure 4.8 (1) shows the layout of one enhanced node domain. It is assumed that one access network is composed of rings of enhanced node domain. Figure 4.8 (2) gives an example of one access network consists of 3 rings of enhanced node domains. And each of the enhanced node domain contains several rings of ARs.
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

Figure 4.8 Network Model: Hexagonal layout. (1) One enhanced node domain consisting of 3 rings of ARs; (2) One access network consisting of 3 rings of enhanced node domains

4.5.2 User Mobility Models

There are two widely used mobility models in the literature: fluid flow model [59] and random walk model [60] [61]. Of the two models, fluid flow model is more suitable for users with high mobility pattern, which means infrequent speed and moving direction changes. Random walk model is more appropriate for pedestrian users, whose mobility pattern is generally limited to certain geographic area, such as residential and business building.
In this section, the fluid flow model and random walk model will be explained in detail.

### 4.5.2.1 Fluid flow model

Fluid flow model is widely adopted to analyze boundary crossing issue, such as handover, in the application of legacy wireless networks providing mainly voice services. Some initial work has been carried out in [62], [63] and [64] making use of the fluid flow model to evaluate the system performance for personal communication systems (PCS). Recently, the fluid flow model has been utilized to analyze location related issues in Mobile IP protocols, such as MIPv6 in [65], HMIPv6 in [66] and [67], the comparison of MIPv6 and HMIPv6 in [68], etc.

In the fluid flow model, it is assumed that the direction of an MN’s movement is uniformly distributed in the range of (0, 2π) [59]. Average speed of an MN is denoted by v. Let \( R_m \) and \( R_n \) be the enhanced node domain crossing rate and the network crossing rate, respectively. Then enhanced node and network crossing rates are given by Eq. 4-2 and Eq. 4-3 respectively,

\[
R_m = \frac{\rho v l_m}{\pi} \tag{4-2}
\]

\[
R_n = \frac{\rho v l_n}{\pi} \tag{4-3}
\]

where, \( l_m \), \( l_n \) and \( \rho \) are the perimeters of an enhanced node domain, a network and MN’s density, respectively. In a network \( C(K) \) consisting of \( K \) rings of enhanced nodes, \( l_n \) is as follows,

\[
l_n = 6 \times (2 K + 1) \times \frac{l_n}{6} = (2 K + 1) l_n \quad (K \geq 1) \tag{4-4}
\]

In [69], the value of perimeter \( l \) is estimated using the formula for the area and circumference of a circle with size \( S \):

\[
l = 2 \sqrt{\pi \cdot S} \tag{4-5}
\]

From Eq. 4-2 and Eq. 4-5, it is derived that,

\[
R_m = \frac{2 \rho v \sqrt{S}}{\sqrt{\pi}} \tag{4-6}
\]

In order to derive the enhanced node crossing rate for a single moving user, Eq. 4-6 is divided by total number of moving users in its area, which is \( \rho S \). Thus,

\[
R_m = \frac{2 v}{\sqrt{\pi S}} \tag{4-7}
\]
Therefore, the movement rate for an MN out of a network can be represented as follows,

$$R_n = \frac{2v}{\sqrt{\pi N(K) S}} \quad \text{Eq. 4-8}$$

where, $S$ is the enhanced node domain area and $N(K)$ is the network domain size (number of enhanced node domains).

### 4.5.2.2 Random walk model

Random walk model is also one of the commonly adopted mobility models. Similar to fluid flow model, the Random walk model has been used to analyze location related signalling cost issues in PCS networks [61] [70] [71]. In HMIPv6 network, the random walk model has also been applied to evaluate the signalling cost, such as BU cost, in [66] [67] and [72].

In random walk model, the next position occupied by an MN is equal to the previous position plus a random variable whose value is drawn independently from an arbitrary distribution [73]. In Figure 4.8, if the MN is located in a cell of $r^{th}$ ring, the probability that a movement will result in an increase or decrease in the distance from the centre is derived as follows,

$$p^+(r) = \frac{1}{3} + \frac{1}{6r} \quad \text{and} \quad p^-(r) = \frac{1}{3} - \frac{1}{6r} \quad \text{Eq. 4-9}$$

![Figure 4.9 State transition diagram for the markov chain model](image)

A Markov chain of $r$ states is defined here, as shown in Figure 4.9. The state $r$ ($r \geq 0$) indicates the distance between the current location of the MN and the centre. Thus, the state is equivalent to the index of a ring in which the MN is located in. For instance, state “3” indicates that MN currently resides in the 3rd ring; the MN is in state $r$ if it is currently residing in ring $r$. The transition probabilities $\alpha_{r,r+1}$ and $\beta_{r,r-1}$ represent the probabilities of MN’s movement from state $r$ to $r+1$, and from state $r$ to $r-1$. They also indicate the distance of the MN from the centre of an access network increases ($r \rightarrow r+1$) and decreases ($r \rightarrow r-1$), respectively. $\alpha_{r,r+1}$ and $\beta_{r,r-1}$ can be represented as below,
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

\[ \alpha_{r,r+1} = \begin{cases} 1-q, & \text{if } r=0 \\ (1-q)\left(\frac{1}{3^{r}}\right), & \text{if } 1 \leq r \leq R. \end{cases} \quad \text{Eq. 4-10} \]

\[ \beta_{r,r+1} = (1-q)\left(\frac{1}{3^{r}}\right), \quad \text{if } 1 \leq r \leq R. \quad \text{Eq. 4-11} \]

where, \( q \) is the probability that the MN remains in the same enhanced node domain. And \( 1-q \) is the probability that the MN moves to another enhanced node domain. \( R \) is the number of rings of enhanced node domains within one access network, for instance, \( R=3 \) in Figure 4.8 (2).

Let \( \pi_{r,R} \) be the steady state probability of state \( r \) within an access network consisting of \( R \) rings of enhanced node domains. By Eq. 4-10 and Eq. 4-11, \( \pi_{r,R} \) can be represented as follows,

\[ \pi_{r,R} = \begin{cases} \frac{1}{1+\sum_{r=1}^{R} \prod_{r=0}^{r-1} \alpha_{r,j+1}} \prod_{r=0}^{r-1} \beta_{r+1,j} \prod_{r=0}^{r-1} \beta_{r+1,j} \pi_{0,R}, & \text{if } 1 \leq r \leq R. \end{cases} \quad \text{Eq. 4-12} \]

Therefore, the probability that the MN leaves the access network is \( \pi_{R,R} \alpha_{R,R+1} \).

4.5.3 Calculation of the Signalling Cost

4.5.3.1 Signalling Cost Using Fluid Flow Model

From Eq. 4-2 and Eq. 4-3, the enhanced node domain crossing rate \( (R_m) \) and the network crossing rate \( (R_n) \) in the fluid flow model are obtained. The location update cost per MN can be derived as follows,

\[ C_{LLU} = \frac{R_n \times C_n + (R_m N_{EN} - R_n) \times C_{EN}}{\rho S_n} \quad \text{Eq. 4-13} \]

where, \( C_n \) and \( C_{EN} \) are the location update cost in the inter access network handover and in the inter enhanced node domain handover. And \( N_{EN} \) is the number of enhanced nodes in one network. \( S_n \) represents the area of the given access network. Since the access network consists of \( N_{EN} \) enhanced node domains, the sum of all enhanced node crossing rate includes the network crossing rate. Therefore, \( R_m N_{EN} - R_n \) is the rate of enhanced node crossing within the access network.

Based on the hexagonal network layout and Eq. 4-1,
\( N_{EN} = 3R^2 + 3R + 1 \) \hspace{1cm} \text{Eq. 4-14}

where, \( R \) is the number of rings the in network model.

\[ S_n = N_{EN} \times S_{EN} = N_{EN} \times \frac{3}{24} \times l_m^2 \] \hspace{1cm} \text{Eq. 4-15}

where, \( l_m^2 \times \sqrt{3}/24 \) is the dimension of a hexagonal enhanced node domain.

Substituting Eq. 4-2, Eq. 4-3, Eq. 4-14 and Eq. 4-15 into Eq. 4-13,

\[ C_{LU} = \frac{\nu l_m C_a + \left[ \nu l_m \times \left( 3R^2 + 3R + 1 \right) \right] \times C_{EN}}{\pi \times \frac{\sqrt{3}}{24} \times \left( 3R^2 + 3R + 1 \right) \times l_m^2} \hspace{1cm} \text{Eq. 4-16} \]

From Eq. 4-4 and \( l_m = (2R+1)l_m \), let \( r = l_m / l_m = 2R+1 \). Thus,

\[ C_{LU} = \frac{\nu r C_a + \left[ \nu \times \left( 3R^2 + 3R + 1 \right) \right] \times C_{EN}}{\pi \times \frac{\sqrt{3}}{24} \times \left( 3R^2 + 3R + 1 \right) \times l_m^2} \hspace{1cm} \text{Eq. 4-17} \]

Since the signalling cost is proportional to the distance of two entities in IP networks \([66]\), the following parameters to calculate the signalling cost are defined:

- \( \tau \): the unit transmission cost in a wired link. It is assumed that the unit transmission cost is the cost for BU to HA.
- \( \kappa \): the unit transmission cost in a wireless link.
- \( D_{x-y} \): the distance between network entity \( x \) and \( y \); and \( D_{x-y} = D_{y-x} \).
- \( PC_x \): the processing cost at network element \( x \).
- \( C_{x-y} \): the coefficient of transmission cost for BU/BA (to HA) from entity \( x \) to \( y \). The coefficient is calculated based on the unit transmission cost.
- \( C_{x-y} \): the coefficient of transmission cost for BU/BA (to CN) from entity \( x \) to \( y \).

In HMIPv6, the MN performs global binding update when it moves across the MAP domains and across networks. The global binding update is a process in which an MN registers its RCoA with the CNs and the HA. Therefore, \( C_n = C_{EN} \), and can be obtained from the below equation,
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

\[ C_s = C_{EN} \]
\[ = \kappa + \tau \times (D_{AR-EN} + D_{EN-HA}) + \tau \times (C'_{HA-EN} \times D_{HA-EN} + C_{EN-AR} \times D_{EN-AR}) + C_{AR-MN} \times \kappa \]
\[ + N_{CN} \times \kappa \times C_{MN-AR} + N_{CN} \times \tau \times (C'_{AR-EN} \times D_{AR-EN} + C_{EN-CN} \times D_{EN-CN}) \]
\[ + N_{CN} \times \kappa \times C'_{AR-MN} + N_{CN} \times \tau \times (C_{EN-AR} \times D_{AR-EN} + C_{CN-EN} \times D_{EN-CN}) \]
\[ + PC_{HA} + N_{CN} \times PC_{CN} + PC_{EN} \]

Eq. 4-18

where, \( N_{CN} \) is the number of CNs that the MN is communicating with.

Let \( S_{HMIp} \) be the security signalling cost per MN for the inter access network handover using the previous mechanism, thus,

\[ S_{HMIp} = (R_s \times C_s) / (\rho \times S_s) \]

Eq. 4-19

where, \( C_s \) is the security cost in the handover between access networks. In order to provide authenticated access control in the previous mechanism, the MN needs to consult the AAAH server. The messages are exchanged in the route of MN\( \rightarrow \)AR\( \rightarrow \)EN\( \rightarrow \)AAAF\( \rightarrow \)AAAH, thus, \( C_s \) can be expressed as follows,

\[ C_s = \kappa \times (S_{11} + S_{12}) + \tau \times (S_{21} + S_{22}) \times D_{AR-EN} \]
\[ + \tau \times (S_{31} + S_{32}) \times D_{EN-AAAF} + \tau \times (S_{41} + S_{42}) \times D_{AAAF-AAAH} \]
\[ + PC_{AR} + PC_{EN} + PC_{AAAF} + PC_{AAAH} + 2 \cdot H_{hash} \]

Eq. 4-20

where, the transmission cost of security signalling in a wireless and wired link between corresponding entities is \( S_{ij} \) times \( \kappa, \tau \) (the transmission cost of BU in the same link), under the previous security mechanism. For example, \( S_{12} \) is the coefficient for the transmission cost from MN to AR, and \( S_{21} \) is for the transmission cost from AR to MN. \( H_{hash} \) is hashing cost.

Let \( S'_{HMIp} \) be the security signalling cost per MN for the inter access network handover using the proposed mechanism, therefore,

\[ S'_{HMIp} = (R_s \times C'_s) / (\rho \times S_s) \]

Eq. 4-21

where, \( C'_s \) is the security cost in the handover between access networks.
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

\[
C'_s = \kappa \times S'_1 + \tau \times S'_2 \times D_{AR-EN} + \tau \times S'_3 \times D_{EN-AAA} + \tau \times S'_4 \times D_{AAASF-AAA} \\
+ \tau \times S'_5 \times D_{AAAASF-AAA} + \tau \times S'_6 \times D_{AAAASF-EN} \\
+ \tau \times S'_7 \times D_{EN-AR} + \kappa \times S'_8 \times D_{AAASF-EN} + \tau \times S'_9 \times D_{AAASF-TargetEN} \\
+ \tau \times S'_{10} \times D_{TargetEN-EN} + S'_{11} \times D_{AAASF-TargetEN} \\
+ 2 \cdot G_{sk} + 10 \cdot H_{hash} + 8 \cdot E_{des}
\]

\[\text{Eq. 4-22}\]

where, \(G_{sk}\) is session key generation cost, \(H_{hash}\) is hashing cost and \(E_{des}\) is encryption/decryption cost using DES. And the transmission cost of security signalling in a wireless and wired link between corresponding entities is \(S'_{ij}\) times of \(\kappa, \tau\) (the transmission cost of BU in the same link), using the proposed security mechanism. \(S'\) and \(S''\) are the coefficients for the transmission cost from AAAH server to target AAAF server and from target AAAF server to target EN, respectively.

Let \(C_{total}\) and \(C'_{total}\) be the total signalling cost using the previous security mechanism and the proposed security mechanism. Thus,

\[
C_{total} = C_{LU} + C_x \quad \text{Eq. 4-23}
\]

\[
C'_{total} = C_{LU} + C'_x \quad \text{Eq. 4-24}
\]

4.5.3.2 Signalling Cost Using Random Walk Model

According to the random walk model presented in the previous section, the probability that an MN leaves the given access network is \(\pi_{R,R+1}\). Hence, the total signalling cost per unit time for the previous security mechanism and the proposed security mechanism can be expressed as follows,

\[
C_{total} = \frac{\pi_{R,R+1} \times (C_x + C_n) + (1 - \pi_{R,R+1}) \times C_{EN}}{\bar{T}} \quad \text{Eq. 4-25}
\]

\[
C'_{total} = \frac{\pi_{R,R+1} \times (C'_x + C_n) + (1 - \pi_{R,R+1}) \times C_{EN}}{\bar{T}} \quad \text{Eq. 4-26}
\]

where, \(\bar{T}\) is average enhanced node domain residence time.

The values of the parameters are shown in Table 1 of Appendix C. Some of the parameter values for analysis are referenced from [65], [66], [72], [74] and [75].
4.6 Simulation Results and Analysis

In this section, performance of the proposed mechanism is compared to the previous mechanism defined in [36], [53] and [76] in terms of signalling cost, using both fluid flow model (section 4.6.1) and random walk model (section 4.6.2). In the previous mechanism, DIAMETER protocol is only used to provide the mobile user authenticated access while it roams across Mobile IP foreign networks, without the key management capacity to establish key between MN and new access network and without establishing trust between neighbouring access networks, as in the proposed mechanism.

4.6.1 Results Using Fluid Flow Model

![Figure 4.10 Impact of MN’s speed on total signalling load (fluid flow model)](image)

The unit signalling cost is defined in section 4.5.3.1 to be the transmission cost of a BU message to HA, and it applies to all the result figures in this section. Figure 4.10 shows the impact of MN’s speed on the signalling cost using fluid flow model. The result shows that the signalling cost increases as MN moves at a faster speed. And the signalling cost for the proposed security mechanism is higher than the previous one. This is because that the previous security mechanism does not involve the key generation/distribution process and the signalling for authentication is only performed between the home network and target access network. However, the proposed security mechanism introduces signalling between the home network and target access network for key distribution. The advantage of the proposed security mechanism is that no extra handover delay is introduced, because the authentication of MN and the establishment/distribution of the keys are performed before MN is connected to the target access network.
Figure 4.11 Impact of R (size of the access network: number of rings) on signalling load, using fluid flow model. (1) Total signalling cost vs R; (2) Ratio vs R, where Ratio = total signalling cost using proposed security mechanism / total signalling cost using previous security mechanism.

Figure 4.11 shows the impact of R (size of the access network in terms of number of rings in hexagonal layout) on signalling cost, using fluid flow model. Figure (1) shows that signalling cost decreases as R increases. This is because larger network size indicates smaller inter-access network handover rate, which results in less inter-access handover signalling cost. The proposed security mechanism introduces more signalling compared to the previous one, however, it is also shown in Figure (1) that the signalling cost gain of proposed security mechanism to previous mechanism decreases as R increases. Figure (2) shows the impact of network size R on the signalling cost.
signalling cost ratio which is defined as $\text{Ratio} = \frac{\text{signalling cost with security mechanism}}{\text{signalling cost with previous security mechanism}}$. As $R$ increases, the ratio gets closer to 1, which indicates the extra security cost introduced by the proposed security mechanism can be neglected for large network size.

### 4.6.2 Results Using Random Walk Model

![Graph 1](image1)

![Graph 2](image2)

Figure 4.12 Impact of $R$ (size of the access network: number of rings) on signalling load, using random walk model. (1) Total signalling cost $\times R$; (2) Ratio $\times R$, where $\text{Ratio} =$ total signalling cost using proposed security mechanism / total signalling cost using previous security mechanism
Figure 4.12 demonstrates the impact of R (size of the access network in terms of number of rings in hexagonal layout) on signalling cost, using random walk model. Figure (1) shows the impact of R on the total signalling cost for previous and the proposed mechanisms, and figure (2) shows the impact of network size R on the signalling cost ratio which is defined as:

\[
\text{Ratio} = \frac{\text{signalling cost with security mechanism}}{\text{signalling cost with previous security mechanism}}
\]

It can be concluded from Figure 4.12 that the extra signalling cost introduced by the proposed security mechanism, comparing to the previous mechanism, can be minimised if large network size is considered. Also, both of figure (1) and (2) demonstrate similar trend as those shown in Figure 4.11.

Figure 4.13 Impact of average residence time in enhanced node domain on total signalling load, using random walk model. (1) R=3; (2) R=3 and R=15
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

Figure 4.13 shows the impact of average residence time in enhanced node domain on total signalling cost. Also, signalling cost generally decreases as average residence time increases. This is because that large residence time in the enhanced node domain suggests the MN moves across domains fewer times in a given time. Therefore, the total signalling cost is less. Figure (1) also demonstrates that proposed security mechanism introduces around 30% more signalling cost than the previous mechanism, due to the fact that more signalling between home network and target network is introduced. Figure (2) shows the impact of network size R on the signalling cost. It can be noticed that signalling cost for larger network size (R=15) is generally smaller than that for smaller sized network (R=3). As shown in Figure (2), the signalling cost gain of proposed security mechanism to previous security mechanism is larger for R=3 than that for R=15. This demonstrates that the proposed security mechanism performs better in a larger sized network.

It is also investigated the sensitivity of the signalling cost to the variance in the enhanced node domain residence time. It is assumed that the enhanced node residence time follows a Gamma distribution. The probability density function (pdf) of a Gamma distribution is as follows,

$$f_{\text{gamma}}(t) = \frac{1}{\Gamma(k) \cdot \theta^k} t^{k-1} e^{-\frac{t}{\theta}} \quad \text{Eq. 4-27}$$

where, $k$ is the shape parameter, $\theta$ is the scale parameter and $\Gamma(k) = \int_0^\infty t^{k-1} e^{-t} dt$. The variance of the Gamma distribution is $k\theta^2$ and the mean is $k\theta$. The Laplace transform of $f_{\text{gamma}}(t)$ can be represented as,

$$F_{\text{gamma}}(s) = (1 + \theta s)^{-k} \quad \text{Eq. 4-28}$$

The residence time in an access network is the sum of total residence time that the MN stays in the enhanced node domains within the network. It is assumed here that the number of enhanced node domains passed by a MN is a random variable $p$ with uniform distribution on $[1, N(R)]$. The probability mass function of an uniform distribution can be expressed as,

$$h(p) = \frac{1}{N(R)} \quad \text{Eq. 4-29}$$

And its $Z$ transform is [70]:

$$H(z) = \sum_{i=1}^{N(R)} h(i)z^i = \frac{1}{N(R)} \cdot (z + z^2 + \ldots + z^{N(R)}) = \frac{1}{N(R)} \cdot \frac{z(1-z^{N(R)})}{1-z} \quad \text{Eq. 4-30}$$
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

Let the pdf of the residence time in the network be $g_{net}(t)$ and its Laplace transform $G_{net}(s)$ is as follows [70],

$$G_{net}(s) = H(z)_{z=F_{conn}(s)} = \frac{1}{N(R)} \cdot (1 + \theta s)^{-k} \cdot \frac{1 - (1 + \theta s)^{-kN(R)}}{1 - (1 + \theta s)^{-k}} \tag{4-31}$$

From the property of the Laplace transform, the first-order moment, i.e., the mean value $ar{t}$ of the residence time in the network, is as follows,

$$\bar{t} = -\frac{\partial G_{net}(s)}{\partial s} \bigg|_{s=0} = \frac{k \theta (N(R)+1)}{2} \tag{4-32}$$

![Figure 4.14 Probability vs signalling cost, using random walk model. The enhanced node domain residence time follows Gamma distribution with mean=4 and variance=4, 8 or 16. Size of network R=3.](image)

In [66] [77], Gamma distribution is used to model the cell residence time because of its flexibility in setting various parameters. It is assumed here that the enhanced node domain residence time follows Gamma distribution with mean=4 and variance=4, 8 or 16. Figure 4.14 shows probability distribution of signalling cost (signalling cost/enhanced node residence time), indicating the impact of variance in the enhanced node residence time. If the enhanced node residence time is with a large variance, a high signalling cost occupies a larger amount of the overall signalling cost compared to the enhanced node residence time with small variance. This is because that larger variance of the enhanced node residence time indicates the probability that an MN remains in the enhanced node domain for a shorter time. In other words, MN is with higher
mobility rate. Figure 4.14 also demonstrates that for the same probability, signalling cost for the proposed security mechanism is larger than for the previous security mechanism.

(1) $R=1$: linear x scale
Chapter 4. An enhanced AAA solution for the authenticated and authorized access control

Figure 4.15 Probability v.s signalling cost (signalling cost/network residence time), using random walk model. The enhanced node domain residence time follows Gamma distribution with mean=4 and variance=4, 8 or 16. And the network residence time is derived using enhanced node domain residence time.

Figure 4.15 shows probability distribution of signalling cost (signalling cost/network residence time), using random walk model. The enhanced node domain residence time follows Gamma distribution with mean=4 and variance=4, 8 or 16. And the network residence time is derived using enhanced node domain residence time as explained before. It is shown in the all of the figures that a high signalling cost occupies a larger amount of the overall signalling cost with larger enhanced node residence time variance value. This is because that larger variance of the enhanced node residence time indicates the probability that an MN remains in the enhanced node domain for a shorter time is higher. In another word, the MN has a higher enhanced node and network crossing rate. Figure 4.15 also demonstrates that for the same probability, signalling cost for the proposed security mechanism is generally larger than for the previous security mechanism. Figure (1) and figure (2) shows the impact of different network sizes: R=1 in (1) and R=2 in (2). Obviously, the signalling cost gain of proposed security mechanism to previous security mechanism is larger in network size R=1 than that in R=2 (comparing figure (1) with figure (2) with linear x scale). This is because smaller network size suggests higher probability of internetwork handovers. Also, it can be observed in figure (1) and (2) (see log x scale) that for the same probability, signalling cost for the proposed security mechanism is larger than for the previous security mechanism.
4.7 Discussions

In section 4.6, the performance of the proposed security mechanism is evaluated using the fluid flow model and random walk model. The proposed solution is compared with the previous security mechanism defined in [36], [53] and [76] in terms of the signalling cost. The signalling cost is evaluated against different parameters, such as speed of the MN, size of the network, etc. The results indicate that the proposed security mechanism generates slightly more signalling cost than the previous security mechanism. There are two reasons for the extra signalling cost:

- The previous security mechanism only provides authenticated access control, without the attempt to generate session keys to be used by the MN and mobility agent. While the proposed security mechanism authenticates the MN and generates key to be used between serving and target EN across access networks and possibly to be used between the MN and EN in the target access network.

- In the proposed security mechanism, messages are exchanged between the AAA infrastructure in the home network and both of the target and serving access network for the purpose of authentication and key distribution. But in the previous solution, message exchange is only performed between AAAH server and target access network to authenticate the MN.

The impact of security mechanism on mobility protocols involves two important factors: signalling cost and handover latency. To minimise the negative impact of security, it is desired that the extra signalling load and handover latency introduced by security mechanism should be minimal. However, there is always a trade-off between these two factors. Although the proposed solution introduces more signalling load, it does not introduce extra handover latency. In the proposed solution, the authentication and key generation/distribution are performed before the MN actually hands over to the target access network. Thus, it does not affect the handover latency and also ensures that the session key is available to be used when MN connects to the target network. However, it takes an extra round-trip-time (RRT) to authenticate the MN under the AAA infrastructure using the previous security mechanism, which inevitably increases the handover latency. More detailed analysis for handover delay is provided in Appendix D. It should also be noted from the results that in large scale networks, the proposed solution achieves very similar performance as the previous security mechanism, in terms of signalling cost.
Chapter 5

5 An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

With the introduction of MAP in HMIPv6, one access network is further divided into domains which are managed by MAP. The mobility management can be localized in one MAP domain, while the procedures for location update is different for handoff across MAP domains. Therefore, handover in HMIPv6 networks can be classified as shown in Figure 5.1:

- Network level handover: The scenario where the MN moves across different access networks.
- Macromobility level handover: The scenario where MN moves within one access network, performing handover across enhanced node domains.
- Micromobility level handover: The scenario where MN moves within one enhanced node domain, performing handover from one AR to another.

![Figure 5.1 Different handoff domains: micromobility level, Macromobility level and network level](image-url)
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

Many existing security issues need to be solved in all of the three handover scenarios. Chapter 4 considers the network level handover by providing solution to authenticate the MN and generate key that can be used later on. Problems remain in the area of micromobility level handover. Among the security issues in the micromobility handoff scenario, the following two problems are essential:

- Authentication of the MN. It is to make sure that it is the authentic MN which is requesting the handover.
- Secure the important mobility signalling. It is required that the key management scheme exists to generate the key for the purpose of securing the mobility signalling, such as BU message.

5.1 Related Work

In order to secure the essential signalling messages, such as BU, it is required to establish SA between two Mobile IP entities. Much progress has been done in securing the global BU/BA messages exchanged between MN and CNs, using return routability procedure defined in [4] and Cryptographically Generated Addresses (CGA) proposed in [78]. However, these solutions are proven to be inefficient against DoS attacks in [79].

With the introduction of local location update in HMIPv6 network, securing local BU/BA messages is necessary as well, although there is not as much work as in securing the global BU/BA messages. In general, there are two methods to secure the handover in HMIPv6: CGA based mechanism and AAA based mechanism.

- CGA based mechanism

CGA is a method for binding a public signature key to an IPv6 address in the Secure Neighbour Discovery Protocol (SEND) [80]. The basic idea is to generate the interface identifier of the IPv6 address by computing a one-way hash of the public key. The resulting IPv6 address is called a CGA. The corresponding private key can then be used to sign messages sent from this address. The other end point can verify the binding between the public key and the address, by re-computing the hash and comparing the result with the interface identifier. Thus, messages sent from the IPv6 address can be secured by attaching the public key and related parameters and by signing the message with the corresponding private key. Mechanisms using GCA work without a certification authority or verification infrastructure [78].

Based on the concept of CGA, some authenticated symmetric key exchange protocols have been proposed in [81] [82] [83]. In [81], it is specified a method that allows the MN to establish
SA with certain MAP. It is proposed in [82] a general method to secure the handover signalling as required in IPv6 handover optimization protocols such as FMIPv6 and context transfer protocol (CXTP) [84]. A mechanism is proposed in [82] to distribute a symmetric handover key for FMIPv6 using Secure Neighbour Discovery (SEND) protocol. All of these solutions are based on the use of CGA technology, thus, the MIP address (such as the MN’s LCoA) is required to be computed based on CGA technology.

- AAA based mechanism

A verification infrastructure is one of the means for authentication and establishment of SA. AAA infrastructure has been proven to achieve good integration with MIP protocols. In Mobile IP networks, AAA infrastructure not only provides authenticated network service to MN roaming in a foreign network, but also functions as a server to generate keys and deliver key/keying materials to the relevant entities.

The reasons why AAA infrastructure is chosen to be used in the proposed solution are,

a. It is to be consistent with the previous solution proposed in chapter 4, which also uses AAA protocol. In order to most re-use the resources, including the “hardware” resources such as network entity, and the “software” resources such as the keys generated in other solution, it is beneficial if all of the solutions can be based on the architectural framework proposed in Figure 3.1.

b. It is to avoid the necessity of introducing CGA technology and unnecessary overhead of computing MIP addresses based on CGA technology.

Much work has been done making use of AAA protocol to secure the MIPv4/v6 signalling [85], while the integration of AAA/HMIPv6 (FMIPv6) remains to be explored. It is proposed in [86], a mechanism to establish handover keys for securing FMIPv6/HMIPv6 signalling using AAA infrastructure. The initial attempt has also been made in [87] to secure the handover in F-HMIPv6 based on the mechanism proposed in [86]. It is defined in [86] a key management protocol to generate handover key between a MN and an AR for the purpose of securing signalling messages in FMIPv6 or any other protocol that requires to establish SA between the MN and the related network entity. The problem with this mechanism is that it introduces too much overhead because of the key generation process. Every time the MN changes the AR, the key generation, which is believed to be a time-consuming process, needs to be executed. In order to reduce the negative impact of the key management scheme on the handover performance, a “lightweight” solution with less signalling overhead involved to generate the handover key is needed. As an improvement for the mechanism proposed in [86], it is proposed in this chapter an enhanced key
management scheme for handover/fast handover in HMIPv6 network to simplify the key generation process.

5.2 Solution Overview

Based on the architectural framework shown in Figure 3.1, it is proposed here an enhanced key management scheme to secure the handover within one enhanced node domain and between enhanced node domains within one access network. It authenticates the MN before the handover takes place and also protects handover by securing the signalling between the two entities involved (MN and AR, or MN and EN) using a handover key (HK) generated in the scheme. The secured handover process includes two procedures: key generation and securing handover messages, such as BU, fast BU, etc. In the proposed solution, making use of the intelligence of the EN, a bunch of keys can be generated at one time and distributed to the entities involved at a later stage. Thus, the signalling overhead and handover latency introduced by key management can be reduced.

5.2.1 Operational Domain and New Terminology

![Diagram of the proposed solution: domain and entities involved]

Figure 5.2 The proposed solution: domain and entities involved

Figure 5.2 illustrates the domain that the proposed solution is operating in and relevant network entities involved in the solution. As shown in the figure, a new network entity, namely handover
key server (HKS), is introduced. In theory, it is the entity that could generate the handover key/keying materials required for securing MIP signalling. In practice, the HKS can be collocated with a AAA server (either AAAF server or AAAH server) in the AAA infrastructure. The HKS interacts with the EN to distribute keys/keying materials.

As introduced in Section 2.1.2.2, the mobility management is localized when MN moves within one enhanced node domain. In order to keep the enhanced node updated with MN's new LCoA when the MN moves between ARs, the local BU/BA messages need to be exchanged between the MN and the enhanced node via AR. It is essential to ensure that it is a legitimate MN requesting the handover service. And at the same time, the location update signalling messages must be secured. Since Mobile IP protocol does not provide a method to establish session keys/related keying materials between the MN and corresponding network entity, a key management protocol needs to be introduced to assist the procedure.

5.2.2 Trust Model

It is assumed that some pre-established SAs exist between some network entities. The trust model is illustrated in Figure 5.3, and explained as follows,

- Between MN and HKS

Serving as a trusted third party, the HKS shares two keys with the MN,

a. A pre-shared handover master key (HMK) exists between the MN and the HKS. The HKS is not for the purpose of securing any signalling messages, as it is only used for derivation of other keys, such as handover key. The method of establishing HMK is out of the scope of the proposed mechanism. However, as part of the AAA infrastructure, there are many ways to establish the pre-shared secrets between the MN and HKS. As mentioned in section 5.2.1, the HKS can be collocated with AAA server. For instance, if the HKS is collocated with the AAAH server, the HMS can be established when MN subscribes to the service (as the key Ks in Chapter 4). If the HKS is collocated with the AAAF server, the HMS can be established in a way described in Chapter 4, when the MN first enters an access network.

b. A handover integrity key (HIK) is also shared between the MN and the HKS. As indicated by its name, it is a key used to provide integrity for messages exchanges between MN and HKS. It is derived from the HMK.

- Between enhanced node and ARs within its domain
As specified in HMIPv6 protocol, the ARs within one MAP domain should assist the MN in selecting the most appropriate MAP and should deliver the RtAdv message sent by the MAP to the MN. Therefore, the secured links must exist between the enhanced node and all ARs located within its domain. It is feasible by using the intelligence of the enhanced node. The enhanced node is configured to have knowledge about its surrounding entities, such as neighbouring enhanced node, the ARs, etc. And the enhanced node is supposed to be able to manage the ARs within its own domain.

![Diagram of Trust Model](image)

**Figure 5.3 Trust Model**

Figure 5.3 also shows the interaction between HKS and enhanced node. Once receiving request from the enhanced node, the HKS should distribute relevant keys/keying materials to the enhanced node as the response. Among the group of ARs within one enhanced node domain, the serving AR should also assist in delivering keying materials to the MN.

### 5.2.3 Assumptions and Requirements

The following assumptions are made:

- **The use of AAA infrastructure**

  It is assumed that AAA infrastructure is used. Based on the key management ability provided by AAA protocol, it is beneficial to use AAA framework for the establishment of handover keys. The HKS, as part of the AAA infrastructure, is collocated with the AAA server. The enhanced node which interacts with the HKS, should be able to function as the AAA client. AAA protocol is used for message exchanges between HKS (AAA server) and the EN (AAA client).

- **Pre-shared secrets**
The proposed solution works based on the existence of pre-shared secrets, as explained in Section 5.2.2. The establishment of the pre-shared keys is outside the scope of the mechanism, although it should be noted that the master key must be refreshed periodically. This is basically to avoid the possibility of compromising the key by analyzing a considerably large amount of traffic.

Some requirements are also explained as follows,

- Minimal impact on MIP protocol

  It is required that the key management procedure should have minimal impact on the mobility protocols. By “minimal impact”, it suggests the proposed solution should not introduce too much handover latency and signalling overhead.

- Freshly generated session keys

  Since AAA-based key management is widely deployed by a variety of standards developed by either IETF or other organizations, guidance for AAA key management is provided by IETF networking group in [88]. It is required by the guidance that the session keys should be strong and fresh. And the session keys should not be dependent on one another. Thus, the compromise of one session key does not lead to the failure of other ones. A fresh cryptographic key is the key generated specifically for only one purpose. The AAA protocol needs to ensure that the keying materials for deriving the session keys are fresh. This is feasible by using a randomly generated value that is used only once, which is usually called the “nonce”. Multiple session keys can be derived from a pre-shared secret and a nonce, thus it is guaranteed that the session keys are fresh.

### 5.2.4 Overview on the key generation procedure

![Figure 5.4 Overview on the key generation procedure](image)
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

Figure 5.4 gives an overview on the basic key generation procedure. The HKS, which cooperates with the MN to generate a HK, is collocated with the AAAF server. The MN, upon attaching to an AR that belongs to a new enhanced node domain, sends a handover key request (HKReq.) message to the AR. The discovery of entering a new enhanced node domain can be done through the RtAdv. message. After validating the MN's CoA, the AR forwards the HKReq. message to its enhanced node. The enhanced node then initiates an AAA request message, encapsulating the payloads of HKReq. message. After successful authentication and authorization using the MAC option which is calculated by the MN using the HIK, the HKS then generates a bunch of HKs for every ARs in its domain and sends an AAA response message over to the EN. All HKs and keying materials are included in the response message. After receiving the AAA response message, the EN can distribute the relevant HK to the corresponding AR in it domain, except for the MN's serving AR. The EN also sends a handover key response (HKResp.) message to the MN's serving AR. In this message, the keying materials for the MN to generate the HKs are included. It also includes the HK for the serving AR. When the MN receives the HKResp. message from the serving AR, it retrieves the keying materials and derives the HKs using the materials. The MN can also authenticate the HKResp. message by validating a MAC option calculated by the HK shared between the MN and the serving AR.

5.3 The Enhanced Key Management Scheme for Securing Handovers in HMIPv6 Networks

5.3.1 Description of the Signalling Details

Continuing with the key generation procedures described in Section 5.2.4, the signalling details illustrated in Figure 5.5 are explained in the following paragraphs. It is assumed that MN enters a new enhanced node domain which has n ARs: $AR_1, AR_2, \ldots, AR_n$, and the MN is about to connect with $AR_1$.

1. The MN sends a handover key request (HK Req.) message to the serving AR ($AR_1$). The HK Req. message includes the following information:

   - MN's CoA, a nonce generated by the MN ($N_{MN}$), the pseudo random function (PRF) algorithm that the MN chooses to use for key generation, the MN's ID ($ID_{MN}$), which is NAI of the MN, a message ID ($ID_{MSG}$) which can identify this message exchange and MN-HKS MAC option.
The MN-HKS MAC option is a MAC of the message field calculated by the MN. The value of the MN-HKS MAC is calculated using the HIK, which is the key derived from the HMK and shared between MN and HKS. Therefore, by validating the MN-HKS MAC option, the HKS can authenticate the MN and perform authorization for the handoffs before deriving the HKs.

2. Upon receiving the HK Req. message, the serving AR (AR₁) needs to verify the MN's CoA carried in the message. If the CoA is valid, AR₁ forwards the HK Req. message to the enhanced node.

3. The enhanced node, as an AAA client, initiates an AAA request message, encapsulating the information in the HK Req. message. Apart from the information in HK Req. message, the following information is added to the AAA request message by the enhanced node:
- the number of the ARs which belong to the enhanced node domain (Num_ARs) and the ID of each AR (ID_AR₁, ID_AR₂, ..., ID_ARₙ), which is the IP address of all ARs as seen by MN.

4. Upon receiving the AAA request message, the HKS should first validate MN-HKS MAC option using the HIK it shares with the MN. If the authentication and authorization is successful, the HKS then proceeds to take the following actions:
   a. The HKS generates a set of HKs/keying materials. A nonce is needed for each of the ARs, thus, n nonces are generated: N_{HKS,1}, N_{HKS,2}, ..., N_{HKS,n}, where N_{HKS,i} (i=1,...,n) denotes the nonce generated for HK between MN and ARᵢ. The nonces will be used in the HK generation correspondingly. The HKS also generates n keys: HK₁, HK₂, ..., HKₙ, since n different session keys are required to be shared between MN and n ARs. Where, HKᵢ (i=1,...,n) is the handover key to be shared between MN and ARᵢ.
   b. The HKS sends a AAA response message to the enhanced node. It includes n nonces generated by the HKS, n freshly generated HKs: HK₁, HK₂, ..., HKₙ, and a result code indicating whether the authentication is successful or not.

5. Upon receiving the AAA response message, the enhanced node should take different actions for the serving AR (AR₁) and all other ARs (AR₂, ..., ARₙ) in its domain.
   a. The enhanced node sends handover key response (HK Reps.) message to the serving AR. The following information is included in this message:
      i. The message ID (ID_{MSGR}) carried in the HK Req. message to identify it is the response to the particular HK Req. message MN initiated.
      ii. The CoA of the MN, which is carried in the HK Req. message.
      iii. The pseudo random function (PRF) algorithm that the HKS uses for key generation.
      iv. The MN's ID (ID_{MN}), as carried in the HK Req. message.
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

v. The result code indicating the result of the HK Req. message.
vi. The SPI that can be used to index every key
vii. The Key/keying materials: the HK for AR₁: HK₁ and all of the nonces that MN needs to derive the HKS: \( N_{HKS,1}, N_{HKS,2}, \ldots, N_{HKS,n} \).

b. The enhanced node also sends the HKS: HK₂, HK₃, ..., HKₙ with its SPI, to the corresponding ARs: AR₂, ..., ARₙ. This can be secured by the SA existed between the EN and all ARs in its domain.

Figure 5.5 Signalling of the enhanced key management scheme for securing the handover process

6. Having received a HK Resp. message with a successful result code, the serving AR (AR₁) stores HK₁ received from the enhanced node. The AR₁ also sends the HK Resp. message to the MN. It includes the following information in this message:

the message ID (ID_MSG), MN's CoA, the PRF which HKS confirms to use for key generation, result code indicating whether HK Request is successful or not, SPIs to index the HKS, the keying
material which MN needs to derive the HKs: \( N_{HKS,1}, N_{HKS,2}, ..., N_{HKS,n} \), and a MN-AR MAC calculated by \( AR_1 \) using \( HK_1 \).

Making use of the keying materials obtained, the MN derives all of the HKs: \( HK_1, HK_2, ..., HK_n \), and validates the MN-AR MAC using \( HK_1 \). Therefore, the group of HKs: \( HK_1, HK_2, ..., HK_n \), is available to secure the future handovers between ARs within this enhanced node domain.

In the proposed scheme, the MN is authenticated and authorized when it first enters an enhanced node domain. The MN now obtains all of the HKs that are possible to be used in the handovers within one enhanced node domain. Therefore, when the MN performs handoff, it is not necessary to generate HK every time the MN changes point of attachment. The HKs can be used to secure the handover signalling between MN-AR-Enhanced Node. The “signalling” here, does not only mean the mobility messages, but also the QoS messages, such as QoS combined BU.

### 5.3.2 Details on Key Derivation

As discussed in section 5.3.1, two types of keys needs to be derived based on the master key shared between MN and the HKS: HIK and HKs. The key generation details will be provided in this section.

An adaptation of pseudo-random function (prf+) defined in [44] is used here as the key derivation method. The function is termed as “Generalized PRF+ (gprf+)” and it is defined in [86] as follows,

\[
gprf+ (\text{key}, \text{string}) = T_1 \mid T_2 \mid T_3 \ldots
\]

where, “\( \mid \)” indicates concatenation ; \( T_1 = \text{PRF} (\text{key}, \text{string} \mid Y) \); \( T_2 = \text{PRF} (\text{key}, T_1 \mid \text{string} \mid Y+1) \); \( T_3 = \text{PRF} (\text{key}, T_2 \mid \text{string} \mid Y+2) \). It continues as many times as needed to compute all required keys. The keys are taken from the output string depending on the length of the key required.

#### 5.3.2.1 Derivation of HIK

The gprf+ is used as follows to derive the HIK as defined in [86] :

\[
\text{HIK} = \text{gprf+} (\text{key}, \text{string});
\]

Input values: key = HMK; string = “Handover Integrity Key”; \( Y = ID_{MSG} \) in hex

The string “Handover Integrity Key” is a 22-character ASCII string without null termination. The value of \( Y \) is the message ID carried in HK Req. message. The use of \( ID_{MSG} \) allows HIK to be different every time the gprf+ is computed. According to the requirements in section 5.2.3, the
session keys should be freshly generated and used only for one purpose. This usually involves a changing parameter "nonce". However, the MN and the HKS only shares the HMK at the stage of HIK generation, it is necessary to involve a changing parameter so that the HIK can be different every time when it is used. The use of IDMSG ensures that the HIK is fresh and new for every HK Req./HK Resp. exchange.

5.3.2.2 Derivation of HK

The gprf+ is also used to derive the HK as defined in [86]. Let $HK_i (i=1, ..., n)$ denote the HK shared between MN and $AR_i$. And $HK_i$ can be derived as follows,

$$HK_i = \text{gprf}+(\text{key, string});$$

Input values: key = HMK; string = $N_{MN} \mid N_{HKS,i} \mid ID_{MN} \mid ID_{AR_i} \mid \text{"Handover Key";} \; Y = 0x0000$

The string “Handover Key” is a 12-character ASCII string without null termination. $N_{MN}$ is the nonce generated by the MN and transmitted to the HKS through HK Req. message. $N_{HKS,i}$ is the nonce generated by the HKS and to be used for generation of $HK_i$. Nonce $N_{HKS,i}$ is communicated to the MN through HK Resp. message. $ID_{MN}$ is the NAI of the MN. And $ID_{AR_i}$ is the IP address of the corresponding $AR_i$.

It can be noticed that among the keying materials, $N_{HKS,i}$ and $ID_{AR_i}$ are the two sets of information which the MN does not own. The $N_{HKS,i}$ is generated by the HKS, and must be transported to the MN through HK Resp. message. However, it might not be necessary to send $ID_{AR_i}$ of all ARs in the enhanced node domain in the HK Resp. message, as this would unavoidably result in large signalling overhead. To solve this problem, the MN can use $ID_{AR_i}$ transmitted in a RtAdv. message. Since RtAdv. message is sent out before the MIP location update signallings, the MN is still able to generate the HK before the handover is performed. It is assumed that SPI is included in the RtAdv. message, so that the MN can figure out which $N_{HKS,i}$ should be used to generate the handover key for particular AR.

It is assumed that the enhanced node maintains a table, as shown in Table 5.1, to index the keys/keying materials. It generates an index table for each MN entering its domain. When the enhanced node receives a HK Req. from a MN, it automatically creates a table of $n \times 5$, where $n$ is the number of ARs in its domain. The enhanced node puts the index number in the first column, and the $ID_{AR_i}$ in the second column. In the AAA request message, the enhanced node should put the the $ID_{AR_i}$ in corresponding AVP in the same sequence as listed in its index table. The HKS generates nonces and HKs for the corresponding AR, and also puts them in the same order in the
AAA response message as $ID_{AR,i}$ in the AAA request message. Therefore, the enhance node would be able to match right nonce and HK to corresponding AR, and put them in the index table. Upon receiving the AAA response message, the enhanced node also allocate SPI for the key/keying materials. As shown in the table, the SPI is placed in the last column. The $SPI_i$ can be used to index corresponding $N_{HKS,i}$ and $HK_i$. The enhanced node does not need to keep record of index table, thus, once the MN leaves the enhanced node domain, the index table for this MN would be deleted.

<table>
<thead>
<tr>
<th>Index</th>
<th>AR’s ID</th>
<th>N_HKS</th>
<th>HK</th>
<th>SPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$ID_{AR,1}$</td>
<td>$N_{HKS,1}$</td>
<td>$HK_1$</td>
<td>$SPI_1$</td>
</tr>
<tr>
<td>2</td>
<td>$ID_{AR,2}$</td>
<td>$N_{HKS,2}$</td>
<td>$HK_2$</td>
<td>$SPI_2$</td>
</tr>
<tr>
<td>3</td>
<td>$ID_{AR,3}$</td>
<td>$N_{HKS,3}$</td>
<td>$HK_3$</td>
<td>$SPI_3$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$n$</td>
<td>$ID_{AR,n}$</td>
<td>$N_{HKS,n}$</td>
<td>$HK_n$</td>
<td>$SPI_n$</td>
</tr>
</tbody>
</table>

Table 5.1 Index table at the enhanced node, which contains $n$ ARs in its domain

### 5.3.3 Syntax and Semantics of the Messages

#### 5.3.3.1 Handover Key Request/Response Message

The HK Request message is initiated by the MN, and forwarded by the serving AR to its enhanced node. In order to carry the HK Req. message, a new type of mobility header needs to be introduced. The format of the mobility header which carries the HK Req. message is similar to that as defined in [86] with minor modification.

```
1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8
Message ID  PRF  Reserved
Care-of-Address
Mobility Options
```

Figure 5.6 Handover Key Request message format
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

The message fields shown in Figure 5.6 are explained as follows,

- **Message ID**: 1-byte value to identify the HK Req. message. And it remains the same in the HK Resp. message.
- **PRF**: a 2 bit field indicating the PRF algorithm that MN advises to use for HIK and HK generation. Different value is assigned to different algorithm. For instance, when PRF field is set to “1”, it suggests HMAC-SHA1 would be used.
- **Reserved**: Reserved field for future use. It is set to 0 if not used.
- **CoA**: 16-byte field containing the MN’s CoA
- **Mobility Options**: This field with variable length might contain one or more mobility options that are defined separately for different purposes. Since HK Req. message needs to carry MN’s Nonce, MN’ ID and the MN-HKS MAC as described in section 5.3.1, three mobility options need to be defined. It is named as Nonce mobility option, MN Identifier mobility option and MAC mobility option, which will be explained in detail in the following sections.

The Handover Key Response message (HK Resp.) message is sent from enhanced node to AR and from AR to MN. In order to carry the HK Req. message, a new type of mobility header needs to be introduced.

<table>
<thead>
<tr>
<th></th>
<th>12345678</th>
<th>12345678</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message ID</td>
<td>F</td>
</tr>
<tr>
<td><strong>Result Code</strong></td>
<td></td>
<td>Lifetime</td>
</tr>
</tbody>
</table>

**Figure 5.7 Handover Key Response message format**

The message fields shown in Figure 5.7 are explained as follows,

- **Message ID**: 8-byte value to identify the message. And it should match the Message ID field sent in the HK Req. message to indicate that it is the response to the HK Req. message.
- **F**: One bit flag to identify the type of HK Resp. message. As HK Resp. messages with different message field are sent from enhanced node to AR and from AR to MN, the type flag is required to identify it. If the type flag is set to 0, it indicates the message is the HK Resp. sent from the enhanced node to the AR. If the type flag is set to 1, it indicates the message is the HK Resp. sent from the AR to the MN.
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

- PRF: a 2 bit field indicating the PRF algorithm that the HKS used for key generation. If the HKS uses the algorithm suggested in the HK Req. message by the MN, the PRF field in the HK Resp. message should be set to the same value as the PRF field in HK Req. message. If the HKS does not use the algorithm proposed by the MN, the value of PRF indicates the algorithm that HKS used. In this scenario, it is mandatory for the MN to use this algorithm. If the key generation algorithm is not agreed, it results a failure in the result code.
- Reserved: Reserved field for future use. It is set to 0 if not used.
- Result Code: One byte field indicating the result of HK request. Value of “0” indicates the success, in terms of authentication and key generation. Other values of the code can be assigned to failure with different reasons, such as authentication of the MN failure, PRF algorithm agreement failure (HKS does not agree to use the PRF algorithm proposed by the MN), etc.
- Lifetime: two bytes field indicating the lifetime (in seconds) of the HKs.
- Mobility Options: This field with variable length might contain one or more mobility options that are defined respectively for different purposes. The HK Resp. message with different “Flag” values contains different mobility options. With Flag value set to 0, the mobility options should at least contain Nonce mobility option to carry the Nonces generated by the HKS and HK mobility option to carry the HK to the serving AR. With Flag value set to 1, the mobility options must at least contain Nonce mobility option to carry the nonces MN needs to generate HKs and MAC mobility option to carry the MN-AR MAC sent from the serving AR to the MN.

5.3.3.2 New Mobility Options

As described in section 5.3.3.1, new mobility options, which are included in the HK Req./Resp. messages, need to be defined. Four different types of mobility options were mentioned: Nonce mobility option, MN identifier mobility option, MAC mobility option and HK mobility option. They will be explained in detail in this section.

1. Nonce Mobility Option

The Nonce mobility option is defined to carry nonce generated by the MN or the HKS. It needs to be included in both of the HK Req. and HK Resp. messages.

The fields of Nonce mobility option shown in Figure 5.8 are explained as follows,

- Type: one-byte field to identify the type of the mobility option: “handover nonce”
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

- Length: two-byte field representing the length (in bytes) of the messages fields excluding “Type” field.
- Subtype: one-byte field indicating the type of Nonce mobility option.
  "0": it carries nonce generated by the MN. It is included in the HK Req. message. In this subtype value, a few fields in the mobility option are not used and set to 0. These fields include “Number”, “SPI Lgth”, “Reserved” and “SPI”.
  "1": it carries a number of nonces generated by the HKS. It is included in the HK Resp. message.
- Number: one-byte field indicating the number of nonces carried in this mobility option. If subtype is set to 1, the value of “number” is 1. If subtype is set to 2, the value of “number” should be equal to the number of ARs in this enhanced node domain.
- SPI Lgth: one-byte field indicating the length of each SPI in bytes. Although the default length of SPI is four bytes, this field allows flexible length of SPI to be chosen by the enhanced node.
- Nonce Lgth: one-byte field indicating the length of each nonce carried in this mobility option.
- Reserved: one-byte reserved field for future use. It is set to 0 if not used.
- SPI: SPI is a four byte security parameter index to identify the key/keying materials.

For instance, particular $SPI_i$ can be used to identify the nonce generated by the HKS to derive $HK_i$ and the handover key $HK_f$. This fields carries all $SPI_i (i=1, ..., n) : SPI_1, SPI_2, ..., SPI_n$, which is used to index the corresponding nonce generated by HKS: $N_{HKS,1}, N_{HKS,2}, ..., N_{HKS,n}$.

- Nonce: this field carries nonce generated either by the MN or the HKS for the purpose of HK generation. With “subtype” set to 1, it carries one nonce generated by the MN. With “subtype” set to 2, it carries $n$ nonces generated by the HKS: $N_{HKS,1}, N_{HKS,2}, ..., N_{HKS,n}$. The $n$ nonces are arranged in the order as the SPIs, so that the nonce can be indexed by corresponding SPI at the MN.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>SPI Lgth</td>
<td>Nonce Lgth</td>
</tr>
</tbody>
</table>

SPI

| Nonce |

Figure 5.8 Nonce mobility option

91
2. MN identifier mobility option

The MN identifier mobility option is used to carry the MN’s ID, which is the NAI. The MN identifier mobility option is defined in RFC 4283 [89], thus, there is no need to introduce new mobility option here. As defined in RFC 4283, the MN-NAI mobility option is used to identify the MN. It uses an identifier of the form "user@realm", with the name of network access identifier (NAI), which is introduced in [90].

3. MAC mobility option

The MAC mobility option is defined to carry the MAC value and related information. In the HK Req. message, it carries the MN-HKS MAC. In the HK Resp. message with “F” value set to 1, the MN-AR MAC needs to be carried in the MAC mobility option. And the MAC mobility option is not included in the HK Resp. message if the “F” value is equal to 0. This mobility option is defined in [86] and can be used here.

```
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Subtype</th>
<th>Reserved</th>
<th>Alg</th>
<th>MAC Value</th>
</tr>
</thead>
</table>
```

Figure 5.9 MAC mobility option [86]

The fields of Nonce mobility option shown in Figure 5.9 are explained as follows,

- **Type**: one-byte field to identify the type of the mobility option: “MAC”
- **Length**: one-byte field representing the length (in bytes) of the mobility option excluding the “Type” field
- **Subtype**: one-byte field indicating the type of MAC this mobility option carries. Value of “0” indicates that it contains the MN-HKS MAC (HK Req. message). And value of “1” means that it contains the MN-AR MAC (HK Resp. message).
- **Reserved**: 5-bit reserved field for future use. It is set to 0 if not used.
- **Alg**: 3-bit field indicating the type of algorithm used for MAC calculation. In order to validate the MAC, the receiver must use the algorithm that the sender used to calculate the MAC. Therefore, it is mandatory for the receiver to use the algorithm indicated in “Alg” field. If the algorithm is not supported at the receiver, the authentication will fail and a failure code will be included in the HK Resp. message. “Alg” value of “1” suggests HMAC-SHA1, which is the default algorithm, was used in the MAC calculation.
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

- MAC Value: this field carries the value of MAC. Two different MAC options may be included in this field: MN-HKS MAC option and MN-AR MAC option. The MN-HKS MAC is calculated using the HIK. And the MN-AR MAC option is calculated using the HK, which is shared by the MN and the serving AR. If HMAC-SHA1 is used as the algorithm, MAC can be calculated as follows,

\[
\begin{align*}
\text{MN-HKS MAC} &= \text{HMAC-SHA1 (HIK, mobility header data)}; \\
\text{MN-AR MAC} &= \text{HMAC-SHA1 (HK, mobility header data)};
\end{align*}
\]

where, mobility header data is the content of corresponding mobility header message up to and including “Alg” field in the MAC mobility option.

4. HK mobility option

The HK mobility option is defined to carry HK from enhanced node to the MN’s serving AR in the HK Resp. message. It only needs to be included in HK Resp. message with “F” value set to 0.

The fields of Nonce mobility option shown in Figure 5.10 are explained as follows,

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>SPI</th>
<th>Reserved</th>
<th>HK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SPI</td>
<td>Reserved</td>
<td>HK</td>
</tr>
</tbody>
</table>

**Figure 5.10 HK mobility option**

- Type: one-byte field to identify the type of the mobility option: “handover key”
- Length: one-byte field representing the length (in bytes) of the mobility option excluding the “Type” field
- SPI: four-byte field to carry the SPI which indexes the handover key carried in this mobility option
- Reserved: two-byte reserved field for future use. It is set to 0 if not used.
- HK: Variable length field that carries the handover key. As the HK Resp. Message is sent from the enhanced node to the serving AR, the HK to be shared between the serving AR and MN is included in this mobility option. It is assumed in section 5.2.2 that SA exists between the enhanced node and all ARs in its domain. To secure the handover key delivery, it could be an encrypted HK that is carried in this field.

93
5.3.3.3 AAA Request/Response Message

The DIAMETER applications extend the DIAMETER base protocol which only defines the minimum requirements for an AAA protocol, by introducing new commands and/or AVPs. As DIAMETER has been engaged in integrating with Mobile IP protocols, many DIAMETER applications, such as DIAMETER Mobile IPv4/IPv6 applications, have been standardized by AAA working group in IETF. Based on the good efforts made on DIAMETER/MIP integrated application, it is promising to involve AAA infrastructure in solving the security issues related to Mobile IP. This is because a large amount of AVPs have been defined in DIAMETER MIPv4/v6 applications, and AAA also provides the ability to introduce new AVPs which can be used to carry specific information. The Diameter protocol is designed to be extensible in terms of defining new AVPs, although reuse of existing AVPs is strongly recommended.

DIAMETER Extensible Authentication Protocol (EAP) application defined in RFC 4072 [91], enables the encapsulation of EAP packets in DIAMETER by introducing new commands and AVPs. Since the definition of new command codes and AVPs must be approved by Internet Assigned Numbers Authority (IANA), it is not desired to go too far on saying that new DIAMETER application is defined for this “handover key distribution” scenario. However, it is believed that DIAMETER can provide the functionality to encapsulate other message and perform authentication.

In the proposed solution, the HKS is supposed to be collocated with AAA server, thus, AAA protocol is used to transport request message from enhanced node to HKS. It is assumed that “DIAMETER-HK-Request” command and “DIAMETER-HK-Response” command exist as the AAA request and AAA response message. In the DIAMETER-HK-Request, it includes the information in the HK Req. message (CoA, N_{MN}, PRF, ID_{MN}, ID_{MSG}, MN-HKS MAC) and the information added by the enhanced that the HKS would need for key generation (N_{ARS}, ID_{AR,i}(i=1, ..., n)). In order to encapsulate the payloads, new AVPs are needed in the DIAMETER-HK-Request command:

- HKReq-Payload AVP: It is used to encapsulate the HK Req. sent from AR to the enhanced node.
- Num-AR AVP: It is used to carry N_{ARS} added by the enhanced node. By checking this AVP, the HKS would be able to decide the number of handover key to be generated for this particular AAA request.
- AR-IP AVP: It is a grouped AVP which is used to carry ID_{AR,i}(i=1, ..., n). ID_{AR,i} is one of the keying materials that the HKS uses to generate HKs between AR_i and MN. As defined in [31],
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

a grouped AVP is an AVP whose data is a sequence of AVPs. Diameter protocol allows AVP values of type 'grouped', which implies that the data field is actually a sequence of AVPs. As it is required that the IP address of each AR within the enhanced node domain needs to be transported to the HKS, a grouped AVP is necessary here.

NAS-IPv6-Address AVP defined in section 9.3.2 of RFC 4005 [92] can be used to carry each ID_{AR,i}. And n of the same types in sequence should be included in the grouped AVP to include all ID_{AR,i}.

In the AAA response message, DIAMETER-HK-Response command is used to carry the following information sent by the HKS to the enhanced node:

PRF, N_{HKS,i}, HK_i, Key Lifetime, Result Code,

Therefore, the DIAMETER-HK-Response command must contain the following AVPs:

- MIP-Algorithm-Type AVP (AVP code 345): It can be used to indicate the algorithm that the HKS used to generate HKs. It is defined in section 9.8 of RFC 4004 [36] and can be reused here to transport "PRF" info from the HKS to the enhanced node.

- MIP-Nonces AVP: It is a grouped AVP which is used to carry nonces generated by the HKS: \text{N}_{HKS,i}. MIP-Nonce AVP (AVP code 335) defined in section 9.12 of RFC 4004 [36] can be used to carry each \text{N}_{HKS,i}. And n of the same types in sequence should be included in this grouped AVP to include all \text{N}_{HKS,i}. Please be noted that the sequence should be in accordance with the sequence of ID_{AR,i} in AR-IP-AVP, so that the enhance node would be match \text{N}_{HKS,i} to the correct AR.

- MIP-Session-Keys AVP: It is a grouped AVP which is used to carry HKs generated by the HKS: HK_i. The HKs can be secured using SA existed in the AAA infrastructure. MIP-Session-Key AVP (AVP code 343) defined in section 9.7 of RFC 4004 [36] can be used to carry each HK_i. Similar to the MIP-Nonces AVP, each AVP to carry particular HK should be placed in a sequence according to the AVPs in AR-IP-AVP.

- MIP-MSA-Lifetime AVP (AVP code 367): It can be used to represent the period of time (in seconds) for which the nonces/HKs are valid. It is defined in section 9.13 of RFC 4004 [36].

- Result-Code AVP (AVP code 268): It is defined in RFC 3588 [31] and can be used to indicate the processing result, such as result of validating MN-HKS MAC, result of HK generation, etc. In this AVP, one value is assigned to indicate "success", and other values are assigned to suggest different reasons of "failure", such as failure to validate MAC, failure to use the PRF algorithm proposed by MN for key generation, etc.
5.4 Analytical Models

In this section, the network model [68] and mobility models [68] used to evaluate the signalling cost of the proposed mechanism will be explained in detail.

5.4.1 Network and Mobility Models

Two different mobility models are used to model the user's mobility pattern: fluid flow model and random walk model as explained in chapter 4. They are used in this section with different network layout to evaluate the performance of the proposed solution.

5.4.1.1 Fluid flow model

Network Layout

In order to analyze the signalling load, the following network model (Figure 5.11) is assumed,

![Network model consisting of two layers of nodes](image)

1. The network is a simple two-layer hierarchical model, as illustrated in Figure 5.11. The first layer has a mesh network topology. The enhanced node is first layer node. The second layer has a tree topology with the depth of 1. The AR, HA and CN are second layer node. The MN, CN and HA are located in different network domains.

2. The link hops between the first layer nodes is $a$, and the link hops between the first and second layer nodes in the same network domain is $b$. The ratio of the network scale is defined to be $r=b/a$.

3. MN is connected to the AR through $w_d$ hops of wireless link. And the unit transmission cost over a wireless link is assumed to be $\kappa$ times of the unit transmission cost over a wired link.
**Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks**

**Markov chain model**

![Markov chain model diagram](image)

Figure 5.12 A continuous-time Markov chain model [68]

Figure 5.12 shows a continuous-time Markov chain model, which describes the movement pattern of an MN. The state of a continuous-time Markov chain model, \( i \) \((i \geq 0)\), is defined as the number of AR domains (subnets) where an MN has stayed within an enhanced node domain. For example, state 2 indicates that MN has stayed in 2 AR domains within a given EN. And the state 0 represents that the MN stays out of the given enhanced node domain. The transition rate \( \alpha_{i,i+1} \) \((i \geq 1)\) represents the MN’s movement rate to a neighbouring AR within a given domain. And the transition rate \( \alpha_{0,1} \) represents the MN’s movement rate to an AR within a given domain from out of this domain. On the other hand, \( \beta_{i,0} \) \((i \geq 1)\) represents the MN’s movement rate to another domain from the given domain. It is also assumed that the MN moves out of a given domain within the maximum of \( K \) movements \((K\) is a finite number).

I assume a fluid flow model, explained in section 4.5.2.1, for the MN’s movement pattern. The parameters used are summarized as follows,

- \( \gamma \): the movement rate for an MN out of an AR domain
- \( \lambda \): the movement rate for an MN out of an AR domain within a given enhanced node domain
- \( \mu \): the movement rate for a MN out of a given enhanced node domain

From Eq. 4-7, the movement rate \( \gamma \) for an MN out of an AR domain can be expressed as,

\[
\gamma = \frac{2v}{\sqrt{\pi S}} \quad \text{Eq. 5-1}
\]

where \( S \) is the AR area. It is assumed that an enhanced node domain is composed of \( N(K) \) ARs, as defined in Eq. 4-1, therefore, the movement rate \( \mu \) for an MN out of a given enhanced node domain is,

\[
\mu = \frac{2v}{\sqrt{\pi N(K)S}} \quad \text{Eq. 5-2}
\]

97
Because the MN moves out of a given enhanced node domain also moves out of an AR domain, the movement rate $\lambda$ for an MN out of an AR within a given enhanced node domain can be derived from Eq. 5-1 and Eq. 5-2 as,

$$\lambda = \gamma - \mu = (1 - \frac{1}{\sqrt{N(K)}})\gamma \quad \text{Eq. 5-3}$$

Therefore, the parameters $\alpha_{i,i+1}$ and $\alpha_{0,1}, \beta_{i,0}$ in Figure 5.12 can be expressed as,

$$\alpha_{i,i+1}(i \geq 1) = \lambda, \quad \alpha_{0,1} = \beta_{i,0} = \mu \quad \text{Eq. 5-4}$$

It is assumed that $\pi_i$ is the equilibrium probability of state $i$. And the following equations can be obtained,

$$\mu \pi_0 = \mu \sum_{i=1}^{K} \pi_i \quad \text{Eq. 5-5}$$

$$\mu \pi_{i-1} = (\lambda + \mu) \pi_i, \quad i = 1 \quad \text{Eq. 5-6}$$

$$\lambda \pi_i = (\lambda + \mu) \pi_{i+1}, \quad 2 \leq i \leq K-1 \quad \text{Eq. 5-7}$$

$$\lambda \pi_{i-1} = \mu \pi_i, \quad i = K \quad \text{Eq. 5-8}$$

By the law of the total probability, the sum of the probabilities of all states is 1. Thus,

$$\pi_0 + \pi_1 + \pi_2 + \ldots + \pi_K = \sum_{i=0}^{K} \pi_i = 1 \quad \text{Eq. 5-9}$$

From Eq. 5-5 and Eq. 5-9, it can be obtained that $\pi_0 = 1/2$.

From Eq. 5-6, Eq. 5-7, Eq. 5-8 and Eq. 5-9, $\pi_i$ can be derived as,

$$\pi_i = \begin{cases} 
\frac{1}{2} & \text{if } i = 0 \\
\frac{1}{2} \left( \frac{\mu}{\lambda + \mu} \right) \left( \frac{\lambda}{\lambda + \mu} \right)^{i-1} & \text{if } 1 \leq i \leq K-1 \\
\frac{1}{2} \left( \frac{\lambda}{\lambda + \mu} \right)^{i-1} & \text{if } i = K 
\end{cases} \quad \text{Eq. 5-10}$$

Substituting Eq. 5-1, Eq. 5-2 and Eq. 5-3 into Eq. 5-10, $\pi_i$ can be expressed as,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

\[ \pi_i = \begin{cases} 
\frac{1}{2} & \text{if } i = 0 \\
\frac{1}{2} \times \left( \frac{1}{\sqrt{N(K)}} \right)^{i-1} \left( 1 - \frac{1}{\sqrt{N(K)}} \right)^{K-i} & \text{if } 1 \leq i \leq K-1 \\
\frac{1}{2} \times \left( 1 - \frac{1}{\sqrt{N(K)}} \right)^{K-i} & \text{if } i = K 
\end{cases} \quad \text{Eq. 5-11} \]

Let \( \phi(K) \) be the average number of ARs that the MN stays within a given enhanced node domain. \( \phi(K) \) can be calculated as follows,

\[ \phi(K) = \pi_1 + 2 \pi_2 + 3 \pi_3 + \ldots + K \pi_K = \sum_{i=1}^{K} i \pi_i \quad \text{Eq. 5-12} \]

Substituting Eq. 5-11 into Eq. 5-12, \( \phi(K) \) can be expressed as,

\[ \phi(K) = \frac{1}{2} \times \left[ \sqrt{N(K)} \left( 1 - \sqrt{N(K)} \right) \left( 1 - \frac{1}{\sqrt{N(K)}} \right)^{K-i} \right] \quad \text{Eq. 5-13} \]

**Signalling Cost**

Based on the mobility model and network model, I derive the signalling load, including the security cost and mobility cost, which is location update cost, generated by an MN during its average domain residence time.

**(1) Mobility Signalling Cost**

In order to derive the mobility signalling cost, I differentiate the location update messages as follows,

- Binding Update (BU), which is generated by MN when it crosses the AR domain.
- Binding Acknowledgement (BA), which is the acknowledgement message for BU or BR message.
- Binding Refresh (BR), which is periodically generated when the binding lifetime expires.

The expressions used in the location update cost calculation are summarized as follows,

- \( L_{HMIP} \): Location update cost in HMIP
- \( BU_{HMIP} \): BU/BA cost in HMIPv6
- \( BR_{HMIP} \): BR cost in HMIPv6
- \( BU_{EN} \): BU/BA cost to register with the enhanced node
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

- $BU_{HA}$: BU/BA cost to register with HA
- $BU_{CN}$: BU/BA cost to register with CN
- $BR_X$: cost for BR sent from entity $X$. For example, $BR_{HA}$ is the cost of BR sent by HA.

The MN sends BU message to HA and CNs when it handovers across the EN domain, while it only updates the EN when it performs handover between ARs within one EN domain. Thus, the BU cost can be derived as follows,

$$BU_{HMIPv6} = \pi_x \times (BU_{EN} + BU_{HA} + N_{CN} \times BU_{CN}) - (\phi(K) - 1) \times BU_{EN} \quad \text{Eq. 5-14}$$

where, $N_{CN}$ is the average number of CNs when an MN moves into out of a given enhanced node domain. The BU cost to EN, HA and CN can be derived as,

$$BU_{EN} = (BW_{BU}^{EN} + BW_{BA}^{EN}) \times b + (BW_{BU}^{EN} + BW_{BA}^{EN}) \times \kappa \times w_d \quad \text{Eq. 5-15}$$

$$BU_{HA} = (BW_{BU}^{HA} + BW_{BA}^{HA}) \times (a + 2b) + (BW_{BU}^{HA} + BW_{BA}^{HA}) \times \kappa \times w_d \quad \text{Eq. 5-16}$$

$$BU_{CN} = (BW_{BU}^{CN} + BW_{BA}^{CN}) \times (a + 2b) + 2 \times (BW_{BU}^{CN} + BW_{BA}^{CN}) \times \kappa \times w_d \quad \text{Eq. 5-17}$$

Here, $BW_{BU}^X$ represents the signalling bandwidth consumption generated by a BU message to entity $x$ (EN, HA or CN), and $BW_{BA}^X$ represents the signalling bandwidth consumption generated by a BA message from entity $x$ (EN, HA or CN) as response to corresponding BU. It is assumed that both of MN and CN are connected to the network through $w_d$ wireless links. And it is also assumed that all of the EN, HA and CN return BA messages to the MN.

The signalling cost for BR messages can be represented as below,

$$BR_{HMIPv6} = BR_{EN} \times \phi(K) \times \frac{t_{sub}}{T_{EN}} + BR_{HA} \times \phi(K) \times \frac{t_{sub}}{T_{HA}} + \delta \times N_{CN} \times BR_{CN} \times \phi(K) \times \frac{t_{sub}}{T_{CN}} \quad \text{Eq. 5-18}$$

And, $BR_X$ can be calculated as below,

$$BR_{EN} = BW_{BR}^{EN} \times b + BW_{BR}^{EN} \times \kappa \times w_d \quad \text{Eq. 5-19}$$

$$BR_{HA} = BW_{BR}^{HA} \times (a + 2b) + BW_{BR}^{HA} \times \kappa \times w_d \quad \text{Eq. 5-20}$$

$$BR_{CN} = BW_{BR}^{CN} \times (a + 2b) + 2 \times BW_{BR}^{CN} \times \kappa \times w_d \quad \text{Eq. 5-21}$$

where, $BW_{BR}^X$ is the signalling bandwidth consumption generated by a BR message sent by entity $x$ (EN, HA or CN). In Eq. 5-18, $T_{EN}$, $T_{HA}$ and $T_{CN}$ are the binding lifetimes for the enhanced node, the HA and the CNs, respectively. $t_{sub}$ is the MN’s average AR residence time. Therefore, the
average rate of sending BR message to the enhanced node is \( \frac{k_{sub}}{T_{EN}} \). Similarly, the average rates of sending BR message to the HA and the CN are \( \frac{k_{sub} \times \varphi(K)}{T_{HA}} \) and \( \delta \times \frac{k_{sub} \times \varphi(K)}{T_{CN}} \), respectively. \( \delta \) is the ratio of an MN's average binding time for the CNs to its average domain residence time.

From Eq. 5-1, \( t_{sub} \) can be expressed as,

\[
t_{sub} = \frac{\sqrt{\pi S}}{2V} \quad \text{Eq. 5-22}
\]

The location update cost is the sum of BU/BA cost and BR cost, thus,

\[
L_{HMIPv6} = BU_{HMIPv6} + BR_{HMIPv6} \quad \text{Eq. 5-23}
\]

Substituting Eq. 5-14 and Eq. 5-18 to Eq. 5-23, the total location update cost can be obtained.

(2) Security Signalling Cost

Let \( S_{pre} \) and \( S_{en} \) denote the security cost in previous security mechanism and in the proposed security mechanism. In the previous security mechanism, handover key request needs to be performed every time the MN changes AR, while it is only performed once when the MN changes the EN domain, in the proposed mechanism. Therefore, \( S_{pre} \) and \( S_{en} \) can be expressed as below, similar to Eq. 5-14:

\[
S_{pre} = \pi_0 \times \left( U^p_{req} + U^p_{resp} \right) + \varphi(K) - 1 \times \left( U^p_{req} + U^p_{resp} \right) \quad \text{Eq. 5-24}
\]

\[
S_{en} = \pi_0 \times \left( U^e_{req} + U^e_{resp} \right) \quad \text{Eq. 5-25}
\]

where, \( U^p_{req} \) and \( U^p_{resp} \) represent the security cost for handover key request and handover key response in previous mechanism. And \( U^e_{req} \) and \( U^e_{resp} \) represent the security cost for handover key request and handover key response in the proposed mechanism.

a. Scenario 1: HKS located in the home domain

If the HKS is located in the home domain, for instance, HKS is collocated with the AAAH server, the parameters in Eq. 5-24 and Eq. 5-25 can be calculated as below,

\[
U^p_{req} = BW^p_{HK Req} \times b + BW^p_{HK Req} \times \kappa \times w_d + BW^p_{HK Resp} \times (a+b) \quad \text{Eq. 5-26}
\]

\[
U^p_{resp} = BW^p_{HK Resp} \times \kappa \times w_d + BW^p_{HK Resp} \times b + BW^p_{HK Resp} \times (a+b) \quad \text{Eq. 5-27}
\]

\[
U^e_{req} = BW^e_{HK Req} \times \kappa \times w_d + BW^e_{HK Req} \times b + BW^e_{HK Resp} \times (a+b) \quad \text{Eq. 5-28}
\]
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

\[
U_{\text{Resp}}^{\text{en}} = BW_{\text{HK Resp}}^{\text{en}} \times \kappa \times \omega_d + BW_{\text{HK Resp}}^{\text{en}} \times b + (N(K)-1) \times BW_{\text{HK Resp}}^{\text{en}} \times b + BW_{\text{AAA Resp}}^{\text{en}} \times (a + b) \\
\text{Eq. 5-29}
\]

where, \(BW_X^{\text{pre}}\) and \(BW_X^{\text{en}}\) represent the signalling bandwidth consumption generated by message \(X\) in the previous mechanism and in the proposed mechanism, respectively. The relevant parameters in Eq. 5-26, Eq. 5-27, Eq. 5-28 and Eq. 5-29 are listed and explained as follows,

- \(BW_{\text{HK Req}}^{\text{pre}}\): signalling bandwidth consumption generated by the HK Req. message (MN \(\rightarrow\) AR and AR \(\rightarrow\) EN) in previous mechanism.
- \(BW_{\text{HK Resp}}^{\text{pre}}\): signalling bandwidth consumption generated by the HK Req. message (AR \(\rightarrow\) MN) in previous mechanism.
- \(BW_{\text{AAA Req}}^{\text{pre}}\): signalling bandwidth consumption generated by the AAA Req. message (EN \(\rightarrow\) HKS) in previous mechanism.
- \(BW_{\text{AAA Resp}}^{\text{pre}}\): signalling bandwidth consumption generated by the AAA Resp. message (HKS \(\rightarrow\) EN) in previous mechanism.
- \(BW_{\text{HK Resp}}^{\text{en}}\): signalling bandwidth consumption generated by the HK Req. message (MN \(\rightarrow\) AR and AR \(\rightarrow\) EN) in the proposed mechanism.
- \(BW_{\text{HK Resp}}^{\text{en}}\): signalling bandwidth consumption generated by the HK Resp. message (serving AR \(\rightarrow\) MN) in the proposed mechanism.
- \(BW_{\text{HK Resp}}^{\text{en}}\): signalling bandwidth consumption generated by the HK Resp. message (EN \(\rightarrow\) serving AR) in the proposed mechanism.
- \(BW_{\text{HK Resp}}^{\text{en}}\): signalling bandwidth consumption generated by the HK Resp. message (EN \(\rightarrow\) other ARs in the EN domain, except for the serving AR) in the proposed mechanism.
- \(BW_{\text{AAA Req}}^{\text{en}}\): signalling bandwidth consumption generated by the AAA Req. message (EN \(\rightarrow\) HKS) in the proposed mechanism.
- \(BW_{\text{AAA Resp}}^{\text{en}}\): signalling bandwidth consumption generated by the AAA Resp. message (HKS \(\rightarrow\) EN) in the proposed mechanism.

b. Scenario 2: HKS located in the visiting domain

If the HKS is located in the visiting domain, for instance, HKS is collocated with the local AAAF server, the parameters in Eq. 5-24 and Eq. 5-25 can be calculated as below,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

\[
U_{\text{Req}}^{\text{pre}} = BW_{\text{HKReq}}^{\text{pre}} \times \kappa \times w_d + BW_{\text{AAReq}}^{\text{pre}} \times b + BW_{\text{HKReq}}^{\text{pre}} \times s_d, \quad \text{Eq. 5-30}
\]

\[
U_{\text{Resp}}^{\text{pre}} = BW_{\text{HKResp}}^{\text{pre}} \times \kappa \times w_d + BW_{\text{HKResp2}}^{\text{pre}} \times b + BW_{\text{AAResp}}^{\text{pre}} \times s_d, \quad \text{Eq. 5-31}
\]

\[
U_{\text{Req}}^{\text{conv}} = BW_{\text{HKReq}}^{\text{conv}} \times \kappa \times w_d + BW_{\text{HKResp}}^{\text{conv}} \times b + BW_{\text{AAResp}}^{\text{conv}} \times s_d, \quad \text{Eq. 5-32}
\]

\[
U_{\text{Resp}}^{\text{conv}} = BW_{\text{HKResp}}^{\text{conv}} \times \kappa \times w_d + BW_{\text{HKResp3}}^{\text{conv}} \times b + BW_{\text{AAResp}}^{\text{conv}} \times s_d, \quad \text{Eq. 5-33}
\]

where, \( s_d \) is number of hops that HKS is located away from the enhanced node. And all the other parameters are the same as explained in scenario 1.

Parameters Value is provided in Table II in Appendix C. Some of the parameter values are from [68].

5.4.1.2 Random walk model

Grid Network Layout

A grid (square) network model [93], as illustrated in Figure 5.13, is considered in the analysis. It is assumed that the coverage of the mobile network is divided into cells and the cells are non-overlapping, with equal size and rectangular shape. Figure 5.13 (1) shows a mobile network model with 3 \( \times \) 3 cells. The central cell is numbered as “0”. And the other cells are labelled by the distance of this cell from the cell “0”. The distance between two cells represents the minimum number of movements that is required for an MN to move from one cell to the other one. Thus, the distance between two cells with coordinates \((x_1, y_1)\) and \((x_2, y_2)\) is \(|x_1 - x_2| + |y_1 - y_2|\), as shown in Figure 5.13 (2). Each cell has four neighbouring cells, to which an MN is possible to move to in one movement.

Figure 5.13 Network Model. (1) Grid Network Model, in which cell is labelled by the distance to the centre cell “0”; (2) Distance between cells with coordinates \((x_1, y_1)\) and \((x_2, y_2)\)

103
I consider the cell of the serving enhanced node of an MN as cell "0". A cell labelled with "i" is the cell that is of distance i away from the centre cell.

I define $P_d^i$ as a $(d + 1) \times (d + 1)$ transition matrix. Element $P_d^i (0 \leq i, j \leq d)$ in the matrix represents the probability of a MN moving from a distance-i cell to a distance-j cell in n movements, where d is the movement threshold. When $n = 1$, $P_d^1$ can be represented as follows,

$$P_d^1 = \begin{bmatrix}
    a_{0,0} & a_{0,1} & a_{0,2} & \cdots & a_{0,d} \\
    a_{1,0} & a_{1,1} & a_{1,2} & \cdots & a_{1,d} \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    a_{d-1,0} & a_{d-1,1} & a_{d-1,2} & \cdots & a_{d-1,d} \\
    a_{d,0} & a_{d,1} & a_{d,2} & \cdots & a_{d,d}
\end{bmatrix} \quad \text{Eq. 5-34}$$

where, $a_{i,j}$ is the probability of moving from distance-i cell to distance-j cell in exactly one movement. Then for $1 \leq n \leq d$, $P_d^n$ can be represented as follows,

$$P_d^n = P_d^1 \times P_d^{n-1} \quad \text{Eq. 5-35}$$

And $P_d^0 (0 \leq j \leq n)$ is the probability that the current AR is of distance j away from the enhanced node after n movements.

In the grid network layout, two different mobility patterns are considered in this section: directional model, in which the mobile user moves towards one direction, and rectangular model, in which the mobile user can move to all of its neighbouring cells. These two random walk models will be explained in detail in the following sections.

**Directional Random Walk model**

Directional walk model [94] is suitable for mobile vehicle users in the "Manhattan" style street layout. It is assumed that a MN moves towards one direction only in the directional model. Therefore, the MN moves to the next cell on its direction with a probability of 1, as illustrated in Figure 5.14 (1). $a_{i,j}$ can be presented as follows,

$$a_{i,j} = \begin{cases} 
1 & \text{if } i+1=j \\
0 & \text{otherwise}
\end{cases} \quad \text{Eq. 5-36}$$

And $P_d^1$ can be expressed as below,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

The state transition diagram for directional model is shown in Figure 5.15 (1). Transition probability from state \(i\) to \(j\) is the probability that the mobile user moves from distance-\(i\) cell to distance-\(j\) cell in one movement. States 0 to \(n-1\) are transient states while state \(n\) is an absorbing state.

![State Transition Diagram](image)

**Figure 5.14** MN’s walk model (1) Directional Walk Model; (2) Rectangular Walk Model; (3) Hexagonal Walk Model

**Rectangular Random Walk Model**

The rectangular random walk model [93] [94], is suitable for pedestrian mobile users. In the rectangular model, a MN moves to one of its four neighbouring cells with equal probability of \(1/4\), as shown in Figure 5.14 (2). \(a_{ij}\) can be presented as follows,

\[
a_{ij} = \begin{cases} 
1 & \text{if } i=0, j=1 \\
\frac{2i+1}{4i} & \text{if } i>0, j=i+1 \\
\frac{2i-1}{4i} & \text{if } i>0, j=i-1 \\
0 & \text{otherwise}
\end{cases}
\]

**Eq. 5-38**

And \(P_d\) can be expressed as below,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

$$P_j = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\
1/4 & 0 & 3/4 & 0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 3/8 & 0 & 5/8 & 0 & \ldots & 0 & 0 & 0 \\
0 & 0 & 5/12 & 0 & 7/12 & \ldots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0
\end{bmatrix}$$

Eq. 5-39

The state transition diagram for rectangular model is shown in Figure 5.15 (2). States 0 to n-1 are transient states while state n is an absorbing state.

Figure 5.15 State diagram for different random walk models. (1) Directional Model; (2) Rectangular Model; (3) Hexagonal Model

**Hexagonal Network Layout**

In the Hexagonal network layout (similar as Figure 4.8) [95] [96], a MN can move to one of its six neighbouring cells with equal probability of 1/6, as shown in Figure 5.14. The MN can also move from one cell to another within the same ring (a ring consists of cells with the same distance to the centre cell). Thus, $a_{ij}$ can be presented as follows,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

\[
a_{ij} = \begin{cases} 
1 & i=0, j=1 \\
\frac{2i+1}{6i} & i>0, j=i+1 \\
\frac{2i-1}{6i} & i>0, j=i-1 \\
\frac{1}{3} & i>0, j=i \\
0 & \text{otherwise}
\end{cases}
\]

Eq. 5-40

And \( P_d^3 \) can be expressed as below,

\[
P_d^3 = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\frac{1}{6} & \frac{1}{3} & \frac{1}{2} & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & \frac{1}{4} & \frac{1}{3} & \frac{5}{12} & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \cdots & \frac{2(d-1)-1}{6(d-1)} & \frac{2(d-1)+1}{6(d-1)} & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1
\end{bmatrix}
\]

Eq. 5-41

Using the concept of rings in the network model, the complex 2-D random walk model can be simplified to a 1-D random walk model. The state transition diagram is shown in Figure 5.15 (3). States 0 is barrier state and state \( n \) is absorbing state. States 2 to \( n-1 \) are transient states. In the state diagram, state \( i \) represents the probability that the MN is in a ring-\( i \) cell. As illustrated in Figure 5.13 (1) and Figure 4.8 (1), the central cell is number as “0”, and the other cells are labelled by the distance of this cell from cell “0”. Thus, ring-\( i \) cell is the cell which is with “\( i \)” distance from the central “0”.

5.4.2 Signalling Cost Analysis

5.4.2.1 Mobility Signalling Cost

The mobility signalling cost here means the location update cost. In HMIPv6, the location update includes the local registration and the global registration. When the MN moves within one enhanced node domain, only local registration to the enhanced node is needed. When the MN moves across enhanced node domain, global registration to HA (possibly CNs) is performed. To calculate the mobility signalling cost, let \( C_l \) be the signalling cost for local registration to the enhanced node, \( C_H \) be the signalling cost for registration to the HA, and \( C_{CN} \) be the signalling cost for registration to the CN.

The following parameters are defined in order to obtain the mobility signalling cost,

- \( k \): distance (number of hops) between HA and enhanced node, as shown in (1) of Figure 5.16.
- \( j \): distance (number of hops) between enhanced node and AR, as shown in (1) of Figure 5.16.
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

- l: average distance (number of hops) between enhanced node and CN, as shown in (1) of Figure 5.16.
- c: average number of CNs that the MN is communicating with while performing handovers.
- δ: transmission cost is assumed to be proportional to the distance between the source and destination entities. And δ denotes the unit transmission cost in a wired link. It is assumed that the unit transmission cost is the cost for local BU to enhanced node.
- m: It is assumed that the transmission cost over a wireless link is m times the cost over a wired link.
- δ_x: transmission cost coefficient for mobility signalling from one entity to another. It is defined as 
  \[ δ_x = \frac{\text{bandwidth consumption for certain mobility signalling in a wired link}}{\text{bandwidth consumption for local BU in a wired link}} \]. The coefficients are listed as follows,
  a. δ_l: transmission cost coefficient for local BA from enhanced node.
  b. δ_h: transmission cost coefficient for BU to HA.
  c. δ_h': transmission cost coefficient for BA from HA.
  d. δ_c: transmission cost coefficient for BU to CN.
  e. δ_c': transmission cost coefficient for BA from CN.
- C_{wireless}: mobility signalling cost over a wireless link between AR and MN.
- C_{ea}: mobility signalling cost between enhanced node and AR.
- C_{he}: mobility signalling cost between HA and enhanced node.
- C_{ce}: mobility signalling cost between CN and enhanced node.
- C_p: processing cost in the mobility agent (i.e., enhanced node) for the mobility signalling.

The registration cost includes the transmission cost and the processing cost of registration signalling.

\[ C_L = C_{wireless} + C_{ea} + 3C_p = mδ + jδ + δ_δ + mδ_δ + 3C_p = (m + j)(1 + δ)δ + 3C_p \] \hspace{1cm} (Eq. 5-42)

\[ C_{he} = C_{wireless} + C_{ea} + C_{he} + 5C_p = mδ_δ + jδ_δ + δ_δ + kδ_δ + δ_δ + mδ_δ + 5C_p \] \hspace{1cm} (Eq. 5-43)

\[ C_{CN} = C_{wireless} + C_{ea} + C_{ce} + 5C_p = mδ_δ + jδ_δ + δ_δ + lδ_δ + δ_δ + jδ_δ + mδ_δ + δ_δ + 5C_p \] \hspace{1cm} (Eq. 5-44)

Let \( Cost_i^L \) denote the average local registration cost for the \( n^{th} \) movement. Then,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

\[ \text{Cost}_t^a = \sum_{j=0}^n P_{0,j} C_L = \sum_{j=0}^n P_{0,j} \left[ (j+m) \cdot (1+\delta) \cdot 3C_p \right] \] \hspace{1cm} \text{Eq. 5-45} \]

where, \( P_{0,j} (0 \leq j \leq n) \) is the probability that the current AR is of distance \( j \) away from the enhanced node after \( n \) movements.

Home registration is performed after the \( d \)th movement to change the enhanced node domain. The average distance between the current enhanced node and the AR after \( d \) movements is

\[ \bar{D}_d = \sum_{j=0}^d P_{0,j} \cdot j \] \hspace{1cm} \text{Eq. 5-46} \]

Let \( \text{Cost}_h^i \) be the cost for home registration and CN registration, then,

\[ \text{Cost}_h^u = (k + m + \bar{D}_d) \cdot (\delta_h + \delta_u) \cdot \delta + 5C_p + c \times \left[ (m + l + \bar{D}_d) \cdot (\delta_c + \delta_e) \cdot \delta + 5C_p \right] \] \hspace{1cm} \text{Eq. 5-47} \]

Let \( \text{Cost} \) denote the average registration cost per movement between enhanced node domains. Since there is one home registration every \( d \) movements and one local registration per movement, then \( \text{Cost} \) can be expressed as,

\[ \text{Cost} = \left[ \sum_{i=1}^d \text{Cost}_h^u + \text{Cost}_t^a \right] / d = \left[ \sum_{i=1}^d \sum_{j=0}^n P_{0,j} \left[ (j+m) \cdot (1+\delta) \cdot 3C_p \right] + (k + m + \bar{D}_d) \cdot (\delta_h + \delta_u) \cdot \delta + 5C_p + c \times \left[ (m + l + \bar{D}_d) \cdot (\delta_c + \delta_e) \cdot \delta + 5C_p \right] \right] / d \] \hspace{1cm} \text{Eq. 5-48} \]

5.4.2.2 Security Signalling Cost

The security signalling cost is analyzed based on Figure 5.16. The security signalling costs using both of the previous and proposed mechanism are evaluated in this section. In Figure 5.16, (1) shows the HMIPv6 domain, on which the mobility signalling cost is evaluated; (2) shows the previous security mechanism, which performs key generation every single time the MN handovers; (3) shows the proposed security mechanism, which only performs key generation when the MN firstly enters a new enhanced node domain.

Previous Mechanism

The security signalling cost means the extra signalling cost introduced by security mechanism. In order to calculate the security signalling cost introduced by the previous security mechanism,
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

let $S_L$ and $S_H$ denote the security signalling cost in local handoff procedures (handover between ARs within a enhanced node domain) and in enhanced node handoff procedures (handover between enhanced nodes), respectively.

![Diagram](image)

**Figure 5.16** Signalling cost. (1) HMIPv6-based network domain; (2) HMIPv6-based network with previous security mechanism; (3) HMIPv6-based network with the proposed security mechanism.

The follows parameters are defined in order to obtain the security signalling cost:

- $S_p$: security processing cost in the mobility agent (i.e., enhanced node) and security entities (i.e., HKS). It is assumed that $S_p$ is two times of $C_p$. 

110
- $S_{ea}$: security signalling cost between AR and enhanced node. Security transmission cost is assumed to be proportional to the distance between the source and destination entities.
- $S_{se}$: security signalling cost between HKS and enhanced node.
- $S_{wireless}$: security cost over a wireless link between AR and MN.
- $s$: distance (number of hops) between enhanced node and HKS, as shown in (1) of Figure 5.16.
- $\delta_{sx}$: transmission cost coefficient for security signalling from one entity to another. It is defined as $\delta_{sx} = \frac{\text{bandwidth consumption for certain security signalling in a wired link}}{\text{bandwidth consumption for local BU in a wired link}}$. The coefficients are listed as follows,
  - $\delta_{s11}$: transmission cost coefficient for security signalling from MN to AR, as shown in (2) of Figure 5.16.
  - $\delta_{s12}$: transmission cost coefficient for security signalling from AR to MN, as shown in (2) of Figure 5.16.
  - $\delta_{s21}$: transmission cost coefficient for security signalling from AR to enhanced node, as shown in (2) of Figure 5.16.
  - $\delta_{s22}$: transmission cost coefficient for security signalling from enhanced node to AR, as shown in (2) of Figure 5.16.
  - $\delta_{s31}$: transmission cost coefficient for security signalling from enhanced node to HKS, as shown in (2) of Figure 5.16.
  - $\delta_{s32}$: transmission cost coefficient for security signalling from HKS to enhanced node, as shown in (2) of Figure 5.16.

Since in the previous mechanism, the key generation is performed every time the MN handovers between ARs, $S_L$ can be expressed as below,

$$S_L = S_{wireless} + S_{se} + S_p + 5S_p = m \cdot (\delta_{s11} + \delta_{s12}) \cdot \delta + j \cdot (\delta_{s21} + \delta_{s22}) \cdot \delta + s \cdot (\delta_{s31} + \delta_{s32}) \cdot \delta + 5S_p$$

Eq. 5-49

Since the security procedure in enhanced node handoff is the same as that in local handoff, using the previous security mechanism, thus, $S_H$ can be expressed as,

$$S_H = S_{wireless} + S_{se} + 5S_p = m \cdot (\delta_{s11} + \delta_{s12}) \cdot \delta + j \cdot (\delta_{s21} + \delta_{s22}) \cdot \delta + s \cdot (\delta_{s31} + \delta_{s32}) \cdot \delta + 5S_p$$

Eq. 5-50

Let $S_L^n$ denote the average signalling cost local cost in local handoff for the $n^{th}$ movement.

Then,

$$S_L^n = \sum_{j=1}^m p_{0,j} S_L + \sum_{j=1}^m p_{0,j} \left[ m \cdot (\delta_{s11} + \delta_{s12}) \cdot \delta + j \cdot (\delta_{s21} + \delta_{s22}) \cdot \delta + s \cdot (\delta_{s31} + \delta_{s32}) \cdot \delta + 5S_p \right]$$

Eq. 5-51
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

Let $S$ denote the average security signalling cost per movement between enhanced node domains. Thus, $S$ can be expressed as,

$$S = \left[ \sum_{i=1}^{d} S_{en,i}^d + S_{u} \right] \frac{1}{d} = \left[ \sum_{i=1}^{d} \sum_{j=1}^{d} P_{en,i,j} \left[ m \cdot (\delta_{s1} + \delta_{s2}) \cdot \delta + s \cdot (\delta_{s31} + \delta_{s33}) \cdot \delta + S_{p} \right] \right] \frac{1}{d}$$

\text{Eq. 5-52}

The Proposed Solution

In the proposed security mechanism, the enhanced node needs to notify all the other ARs (except for the serving AR) the generated HK, when an MN first enters an enhanced node domain. And no any other security signalling are required in the local handoffs within this enhanced node domain afterwards.

The follows parameters are defined in order to obtain the security signalling cost,

- $S_{en}$: security signalling cost between serving AR and enhanced node.
- $S_{HR}$: security signalling cost from enhanced node to all the other ARs except for the serving AR, which is the cost for distributing handover key to the ARs.
- $S_{se}$: security signalling cost between HKS and enhanced node.
- $S_{wireless}$: security cost over a wireless link between AR and MN.
- $\delta_{en}$: transmission cost coefficient for security signalling from one entity to another. The coefficients are listed as follows,
  - $\delta_{s11}$ transmission cost coefficient for security signalling from MN to AR, as shown in (3) of Figure 5.16.
  - $\delta_{s12}$: transmission cost coefficient for security signalling from AR to MN, as shown in (3) of Figure 5.16.
  - $\delta_{s21}$: transmission cost coefficient for security signalling from serving AR to enhanced node, as shown in (3) of Figure 5.16.
  - $\delta_{s22}$: transmission cost coefficient for security signalling from enhanced node to serving AR, as shown in (3) of Figure 5.16.
  - $\delta_{s2n}$: transmission cost coefficient for security signalling from enhanced node to all the other ARs in its domain except for serving AR, as shown in (3) of Figure 5.16. This coefficient stands for the cost of distributing the HK to corresponding AR.
  - $\delta_{s31}$: transmission cost coefficient for security signalling from enhanced node to HKS, as shown in (3) of Figure 5.16.
• $\delta_{32}':$ transmission cost coefficient for security signalling from HKS to enhanced node, as shown in (3) of Figure 5.16.

Let $N$ be the number of ARs in the enhanced node domain. Therefore,

$$N = \begin{cases} 
1 + \sum_{i=1}^{4} 4i = 2r^2 + 2r + 1 & \text{rectangular layout} \\
1 + \sum_{i=1}^{6} 6i = 3r^2 + 3r + 1 & \text{hexagonal layout} 
\end{cases} \quad \text{Eq. 5-53}$$

where, $r$ is the number of rings in the network model. Therefore, the enhanced node needs to notify $N-1$ ARs the corresponding handover key, as shown in Figure 5.16 (3).

Let $\lambda$ denote the proportional constant of the security signalling cost to the distance between enhanced node and ARs (for the delivery of HKs from enhanced node to corresponding AR). Thus, $\lambda = \delta_{32n} \times \delta$.

And, $S_{HK}$ can be expressed as,

$$S_{HK} = \lambda \cdot 1 \cdot N_1 + \lambda \cdot 2 \cdot N_2 + \ldots + \lambda \cdot r \cdot N_r \quad \text{Eq. 5-54}$$

where, $N_r$ is the number of ARs in ring $r$. And, $N_r$ can be expressed as follows,

$$N_r = \begin{cases} 
4i & \text{rectangular model} \\
6i & \text{hexagonal model} 
\end{cases} \quad \text{Eq. 5-55}$$

Therefore,

$$S_{HK} = \begin{cases} 
\frac{\lambda \cdot r(r+1)}{2} & \text{directional model} \\
2\lambda \cdot \frac{r(r+1)(2r+1)}{3} & \text{rectangular model} \\
\lambda \cdot r(r+1)(2r+1) & \text{hexagonal model} 
\end{cases} \quad \text{Eq. 5-56}$$

where, $r$ is the number of rings in the network.

Let $S'_H$ denote the security signalling cost in enhanced node handoff procedure (handover between enhanced nodes). And, $S'_H$ can be expressed as,

$$S'_H = S'_{wreens} + S'_{ea} + S'_{re} + 5S'_p + S_{HK} = m \cdot (\delta'_{S11} + \delta'_{S12}) \cdot \delta + \bar{D}_a \cdot (\delta'_{S21} + \delta'_{S22}) \cdot \delta \\
+ s \cdot (\delta'_{S31} + \delta'_{S32}) \cdot \delta + 5S'_p + (N-1) \cdot S'_p + S_{HK} \quad \text{Eq. 5-57}$$
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

It should be noted that no any security signalling are involved in the local handoffs within the enhanced node domain. Let $S$ denote the average security signalling cost per movement between enhanced node domains. $S = S_H'/d$.

Values of the parameters are provided in Table III in Appendix C.

5.5 Simulation Results

In this section, performance of the proposed mechanism is evaluated against the previous scheme proposed in [86], in terms of signalling cost.

5.5.1 Fluid Flow Model

![Diagram](image)

Figure 5.17 $\varphi(K)$ as a function of $K$. $\varphi(K)$ is the number of an MN's movements within a given enhanced node domain.

$\varphi(K)$, which is the average number of ARs that the MN stays within a given enhanced node domain, is plotted in Figure 5.17 as a function of $K$. As illustrated in this figure, unless $K$ is much smaller than domain size $N$ ($N=20$, 30 or 40), $\varphi(K)$ is rarely sensitive to the change of $K$. Thus, in order to simplify the analysis, it is assumed that $K$ is equal to $N$ ($N=20$).

Ratio of the network scale is defined to be $r=b/a$. Thus, larger $r$ indicates smaller distance between the foreign network and home network. The signalling cost is calculated by the accumulative signalling bandwidth consumption in bytes:

$$\text{Signalling bandwidth in bytes} \times \frac{\text{number of link hops}}{\text{an MN's average domain residence time}}$$

114
Figure 5.18 Impact of $r=b/a$ on signalling cost, with HKS located in another domain. Parameters: $N=20$; $v=20 \text{ km/hr}$; $S=10 \text{ km}^2$; HK size (1) 128 bits (2) 256 bits

Figure 5.18 shows the impact of $r$ on the signalling cost in HMIPv6, HMIPv6 with previous security mechanism and HMIPv6 with enhanced security mechanism. It is assumed that HKS is located away from the enhanced node in another domain, and different HK sizes are considered: HK=128 bits in figure (1); HK=256 bits in figure (2). As illustrated in both of (1) and (2) Figure 5.18, signalling cost decreases as $r$ increases, because smaller distance between home network and foreign network indicates less signalling cost, as the registration cost to HA/CN and security signalling cost to the HKS are smaller. As shown in (1), if HK size is 128bits, the signalling cost of enhanced security mechanism is generally smaller than that of previous security mechanism. Also, the signalling cost gain (signalling cost in enhanced security mechanism-signalling cost in previous security mechanism) is larger when smaller $r$ is considered. This is because that key generation takes place every time when MN changes AR in the previous security mechanism,
thus, the signalling cost is higher when HKS is in another domain that is far away from the visiting domain. As shown in (2), if HK size is 256 bits, the signalling cost of enhanced security mechanism is generally close to that of previous security mechanism. This is because that, in the enhanced security mechanism, distributing all of the HKs with large key size to corresponding ARs introduces more signalling overhead. However, it can be noticed that the signalling cost in enhanced security mechanism is slightly smaller than that in previous security mechanism when \( r \) is small, and when \( r \) is large, the signalling cost in enhanced security mechanism can even becoming a little bit larger than that in previous security mechanism. This is because the HKs are generated by the HKS, thus if the HKS is far away from the visiting domain, distributing HKs and keying materials will introduce more signalling overhead.

![Figure 5.19](image_url)

**Figure 5.19** Impact of \( r=b/a \) on signalling cost, with HKS located in another domain. Parameters: \( N=20 \); HK size=128 bits; \( v=5 \) or 20 km/hr; \( S=10 \) km²

Figure 5.19 the impact of \( r \) on the signalling cost under different MN’s average moving speed \( v=5 \) km/hr and \( v=20 \) km/hr. The impact of \( r \) is similar to that shown in (1) Figure 5.18. And it can be noticed that the signalling cost with \( v=5 \) is generally higher than the signalling cost with \( v=20 \). Because when the number of MN’s movements (handovers) is fixed, if the MN is moving at a low speed, more signalling traffic is generated by the periodic BR messages. Within a certain network residence time, there are more BR messages generated with a lower moving speed.
Figure 5.20 Impact of MN's average speed \( v \) on signalling load, with HKS located in another domain and in the visiting domain \((s=2)\) hops away from the enhanced node). Parameters: \( N=20; \) HK size =128 bits; \( S=10 \text{ km}^2; \) \( r=0.2\)

Figure 5.20 shows the impact of MN's moving speed \( v \) on signalling cost. And two scenarios are considered: HKS is in another domain; HKS is in the visiting domain and it is \( s \) \((s=2)\) hops away from the enhanced node. The result shows that the signalling cost decrease as \( v \) increases. The reason has been explained in Figure 5.19. As \( v \) increases, the number of BR messages decreases, therefore, the total signalling cost during the average network residence time decreases. The result also shows that signalling cost generally is lower when HKS is located in the visiting domain than in another domain, for both security mechanisms. This is because that the security signalling traversing different domains would result in more signalling overhead. It is also illustrated in Figure 5.20 that the proposed security mechanism outperforms the previous mechanism by introducing less overhead, when HKS is located in another domain. And the propose mechanism gives similar performance (neglectably more) to the previous mechanism, when HKS is in visiting domain with \( s=2 \) hops away from the enhanced node. The HKS has to be involved every single time MN performs handover in the previous mechanism, thus, the location of HKS affects the previous mechanism more. However, the proposed mechanism is not as sensitive to the location of HKS as the previous mechanism, since the HKS is only contacted once when MN crosses the enhanced node domain. The reason why the propose mechanism gives similar performance to the previous mechanism when the HKS is located in the visiting domain, is that the keys/keying materials distribution introduce more signalling overhead, although the HK generation is performed less often in the proposed mechanism.
Figure 5.21 Impact of domain size \( N \) on signalling cost, with HKS located in another domain and in the same domain (\( s=2 \) hops away from the enhanced node). Parameters: \( v=20 \text{ km/hr} \); HK size \( =256 \text{ bits} \); \( S=10 \text{ km}^2 \); \( r=0.2 \)

Figure 5.21 shows the impact of domain size \( N \) (number of ARs in one enhanced node domain) on signalling cost. The signalling cost generally increase as the domain size gets larger, as larger domain size means more possible handovers within the domain which would result in more registration signalling and security signalling. As illustrated in Figure 5.21, the signalling cost in the proposed security mechanism is relatively more sensitive to the increase of domain size. Because it is chosen here HK length=256 bits, the distribution of the HKs dominates the security signalling.

(1) HKS is located in the visiting domain, with \( s=1, 2 \) or 5 hops away from EN
Figure 5.22 Impact of HK size on signalling cost. Two scenarios are considered: HKS is in the same visiting domain and it is s (s=1, 2 or 5) hops away from the enhanced node, as in figure (1); HKS is in another domain (etc, home network), as in figure (2).

Figure 5.22 shows the impact of HK size on the security signalling cost. Two scenarios are considered: HKS is in the same visiting domain and it is s (s=1, 2 or 5) hops away from the enhanced node, as in figure (1); HKS is in another domain (etc, home network), as in figure (2). Different key sizes are considered: DES-56bits, 3DES-56bits, 112bits or 168bits, AES-128bits, 192bits, or 256bits, as marked in the figures with black text arrows. As illustrated in the figure (1), the signalling cost is smaller if HKS is placed closer to the enhanced node, which means smaller s value. And, the signalling cost generally increases when larger HK size is chosen. It is also illustrated that the signalling cost produced by the proposed security mechanism is generally more sensitive to the change of HK size, compared to the previous mechanism. This is because that in the proposed solution, the HK/keying materials would be distributed once to all relevant entities. The distribution of keys/keying materials would also result in more signalling cost, if the HKS is with moderate distance away from the enhanced node(s=1 and s=2 in figure (1)). If the HKS is located further away from the enhanced node (s=5 in figure (2)), the proposed scheme introduce less signalling overhead when smaller key size is chosen (3DES-56, 3DES-112 and AES-128). However, if larger key size is considered (3DES-168, AES-192 and AES-256), the proposed mechanism would still introduce more signalling cost, this is because that large keys transmitted over multiple hops (s=5) would result in more signalling overhead. Figure (2) shows the impact of HK size on the signalling cost, if the HKS is located in another domain, rather than
the visiting domain. It is clearly demonstrated that the proposed mechanism generally introduces less signalling overhead than the previous mechanism, no matter what size of the key is considered. However, more gain is achieved, if small key size is chosen (e.g., 3DES-56). The reason why the previous mechanism introduces more signalling cost is the interaction with the HKS located far away in another domain every time the MN performs handover.

![Graph](image)

**Figure 5.23** Impact of $r_s=b/s$ on signalling load, with HKS located in the visiting domain ($s$ hops away from the enhanced node). Parameters: $N=20$; $b=10$; HK size=128 bits.

Ratio $r_s = b/s$ is defined to evaluate the location of HKS, when it is located in the visiting domain. Larger $r_s$ indicates that HKS is located closer to the enhanced node. Figure 5.23 shows the impact of $r_s$ on the security signalling cost. The signalling cost introduced by security mechanisms generally decrease as $r_s$ increases, as shown in the figure. Thus, it is always recommended that HKS should be better collocated with the enhanced node, or at least as close to the EN as possible. The result also shows that the proposed security mechanism would introduce more signalling overhead, because of the distribution of keys/keying materials to all ARs. And the signalling cost gain (signalling cost in proposed mechanism-signalling cost in previous mechanism) increases as $r_s$ gets larger. This is because that the previous mechanism is more sensitive to the location of HKS, as the security related signalling has to go to the HKS every time handover is performed.
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

![Diagram](image)

(1) Previous Security Mechanism

![Diagram](image)

(2) Proposed Security Mechanism

Figure 5.24 Impact of $r = b/a$ and $r_s = b/s$ on $R = \frac{\text{Security Signalling}/(HMIP Signalling + Security Signalling)}{\text{HMIPv6 Signalling cost + security signalling cost}}$, with HKS located in visiting domain ($s$ hops away from the enhanced node). (1) Previous security mechanism; (2) Proposed security mechanism. Parameters: $N=20$; HK size=128; $v=20$ km/hr; $S=10$ km$^2$; $b=10$

Ratio $R = \frac{\text{security signalling cost}}{\text{HMIPv6 signalling cost + security signalling cost}}$ is defined, thus, larger $R$ indicates that the security signalling occupies bigger percentage in the overall signalling and also suggests more security signalling cost. Figure 5.24 shows the impact of ratios $r$ and $r_s$ on $R$, when the HKS is located in the visiting domain, for previous mechanism (figure (1)) and proposed mechanism.
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

(figure (2)). Comparing (1) and (2) in Figure 5.24, the value of R in previous security mechanism (Figure (1)) is generally smaller than in proposed security mechanism (Figure (2)). Thus, the security signalling cost is higher in the proposed security mechanism than that in the previous mechanism. It can be also observed that figure (1) and (2) illustrate similar trend: larger $r_2$ results in smaller value of $R$ and smaller $r$ results in smaller value of $R$. The reason is that as $r_2$ increases, security signalling cost decreases which results in smaller $R$ (smaller security signalling cost results in smaller $R$). And also as $r$ increases, HMIPv6 mobility signalling cost decrease which results in larger $R$ (smaller mobility signalling cost means larger $R$). Larger value of $r_2$ and smaller value of $r$ would bring on smaller value of $R$, which indicates that the security signalling takes less percentage of the overall signalling cost.

5.5.2 Random Walk Model

In this section, the signalling cost is evaluated against the movement threshold $d$, which is the number of handovers the MN performs before it leaves a given EN domain. The signalling cost unit is the cost of transmitting a local BU to EN, as defined in section 5.4.2.1.

5.5.2.1 Directional Model

Figure 5.25 shows signalling cost vs. $d$, in directional walk model. Figure (1) illustrates registration cost in HMIPv6 with different $k$, which is the distance between enhanced node and HA. Large $k$ indicates that MN is far away from its home network, therefore, the registration cost is high. It can also be noticed that the registration cost is very high with small $d$ value and is slightly increasing as $d$ increases when large values of $d$ are selected. This is because small value of $d$ suggests often inter enhanced node handovers which would result in more registration to the home network. And as $d$ gets larger, it suggests MN stays in the enhanced node longer, which would increase the local registration cost. Figure (2) shows total signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. The total signalling cost using the proposed security mechanism is higher than that using previous security mechanism when $d$ is small. This is because smaller $d$ indicates more frequent handoffs between enhanced node domains, in which case the large signalling cost for distributing HKs/keying materials to all ARs and MN in the proposed security mechanism dominates the total signalling cost. It can be also observed from figure (2) that the total signalling cost in the proposed security mechanism gets smaller than that in the previous security mechanism when $d$ increases. This is because larger value of $d$ suggests that MN performs more handoffs within one enhanced node domain, thus, the handover key generation needs to be
performed every time MN handovers to new AR in the previous mechanism. However, no more key generation needs to be performed in the proposed solution, unless the MN leaves the current enhanced node domain. It is demonstrated the figure (2) that the proposed security mechanism performs better when MN stays longer within one enhanced node domain.

![Figure 5.25](image)

**Figure 5.25** Signalling cost in directional walk model. (1) registration cost in HMIPv6; (2) total signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. $K$ is the distance between HA and enhanced node.
An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

Figure 5.26 Impact of threshold (d) on cost ratio in directional walk model. The ratio is defined as:
\[ R = \frac{\text{total signalling cost in HMIPv6 with security mechanism}}{\text{registration cost in HMIPv6}} \]

The cost ratio is defined as: \( R = \frac{\text{total signalling cost in HMIPv6 with security mechanism}}{\text{registration cost in HMIPv6}} \). If \( R \) is closer to 1, it means less security signalling cost comparing to the mobility signalling cost. Figure 5.26 shows the impact of threshold (d) on cost ratio in directional walk model. The result shows that cost ratio decreases and gets close to one as d increases, in the proposed security mechanism. And the cost ratio increases as d increases, with previous security mechanism. This is because that HKs are distributed at one time once MN enters an enhanced node domain, in the proposed mechanism. If MN performs more handovers within this enhanced node domain, the proposed mechanism would be more beneficial. It can be also noticed that smaller K results in larger cost ratio, because smaller k means lower registration cost in HMIP.
5.5.2.2 Rectangular Model

![Graph showing signalling cost in rectangular walk model](image)

**Figure 5.27** Signalling cost in rectangular walk model. (1) registration cost in HMIPv6; (2) signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. K is the distance between HA and enhanced node.

Figure 5.27 shows signalling cost vs. d, in rectangular random walk model with different values of k. Figure (1) and figure (2) demonstrates similar trend as Figure 5.25, although the signalling cost are not as sensitive to the increase of threshold (d) as in Figure 5.25. And the signalling cost is generally less comparing to the cost shown in Figure 5.25, except for the situation when very small value of d is chosen for the proposed security mechanism. This is because that it is less possible that the MN moves far away from the enhanced node as d increase, in rectangular model.
than in directional model. In directional model, as MN moves on, it gets further away from the enhanced node. And in rectangular model, as MN moves on, it could get closer to the enhanced node, from outer ring back to inner ring (such as ring 3 to ring 2). Thus, the mobility signalling to enhanced node and the security signalling to HKS would both reduce, in rectangular model. However, the proposed mechanism introduces a lot more signalling overhead when d is small (figure (2)). The reason is that the HKS has to distribute HKs/keying materials to a large amount of ARs in the enhanced node domain. With the same number of rings, the domain size (number of ARs in one EN domain) in a rectangular model is larger than the size in directional model. It is also demonstrated the figure (2) that the proposed security mechanism performs better when MN stays longer within one enhanced node domain.

Figure 5.28 Impact of threshold (d) on cost ratio in rectangular model. The ratio is defined as:

\[
\frac{\text{total signalling cost in HMIPv6 with security/registration cost in HMIPv6}}{\text{previous security mechanism K=5}}
\]

Figure 5.28 shows the impact of threshold (d) on cost ratio in rectangular random walk model. It demonstrates similar trend as Figure 5.26, although cost ratios are generally higher than in Figure 5.26. The registration cost for HMIP is lower in rectangular random walk model than in directional walk model. The security cost with the proposed security mechanism is higher in rectangular random walk model than in directional walk because the domain size is larger in rectangular model and it costs more to distribute the HKs to every ARs in the domain. The security cost with previous security mechanism is lower in rectangular random walk model than in directional walk model because MN is less possible to be far away from enhanced node in rectangular model than in directional model and it costs less to generate HK every time MN moves. Based on the analysis, it is obvious that the cost ratios are generally higher in rectangular model than in directional model.
5.5.2.3 Hexagonal Model

Figure 5.29 Signalling cost in hexagonal random walk model. (1) registration cost in HMIPv6; (2) signalling cost (mobility signalling and security signalling) in HMIPv6 with previous security mechanism and the proposed security mechanism. K is the distance between HA and enhanced node.

Figure 5.29 shows signalling cost v.s d, in hexagonal random walk model with different k. Figure (1) and figure (2) demonstrates similar trend as Figure 5.25 and Figure 5.27, although all of the signalling cost are less sensitive to the increase of threshold (d) as in Figure 5.27. And figure (2) especially shows that the signalling cost using the proposed security mechanism when d is with small value, is much higher, comparing to the results in Figure 5.25 and Figure 5.27. This
is because that the domain size in hexagonal model is larger than in rectangular model, with same number of rings. Therefore, the signalling cost to distribute HKs/keying materials to every AR is higher in hexagonal model than in rectangular model.

![HMIPv6 with Security Mechanism in Hexagonal Model](image)

**Figure 5.30** Impact of threshold (d) on cost ratio in hexagonal walk model. The ratio is defined as: total signalling cost in HMIPv6 with security/registration cost in HMIPv6.

Figure 5.30 shows the impact of threshold (d) on cost ratio in hexagonal random walk model. It demonstrates similar trend as Figure 5.26 and Figure 5.28, although cost ratios in hexagonal model are generally higher than those in rectangular model, and of course directional model. The reason is similar as the explained in Figure 5.28.

### 5.6 Discussions

In section 5.5, the performance of the proposed security mechanism is evaluated using the fluid flow model and random walk model. The proposed solution is compared with the previous security mechanism in terms of the overall signalling cost. The signalling cost is evaluated against different parameters, such as speed of the HK size, location of the HKS, enhanced node domain size, etc. The results indicate that the proposed security mechanism generates about 10%-50% more signalling cost than the previous security mechanism depending on the scenarios, if the HKS is located in the visiting domain. And if the HKS is located in another domain, rather than the visiting one, the proposed solution can result in less signalling overhead, depending on the distance between the two domains. The main reason why the proposed solution could bring on more signalling cost is the distribution of a bunch of keys/keying materials to all of the ARs/MN. Any of the following situations can increase the signalling cost:
Chapter 5. An Enhanced Key Management Scheme for Securing Handover/Fast Handover in HMIPv6 Networks

- Large domain size (number of ARs in one enhanced node domain).
- Large size key is chosen
- HKS is located far away from the enhanced node
- MN performs limited number of handoffs within the enhanced node domain and leaves the domain quickly. In this case, lots of HK might not be used, and the previous security mechanism outperforms the proposed solution by introducing considerable less signalling overhead.

It can be also concluded that the better scenario for using the proposed security mechanism is that MN stays in the serving enhanced node domain for longer period and the HKS is collocated with or located close to the enhanced node. Moderate enhanced node domain size and key size are also preferred.

The impact of security mechanism on mobility protocols involves two important factors: signalling cost and handover latency. To minimise the negative impact of security, it is desired that the extra signalling load and handover latency introduced by security mechanism should be minimal. However, there is always a tradeoff between these two factors. Although the proposed solution could introduce more signalling load in some of the scenarios, it is obvious that it is beneficial in terms of introducing less handover latency. When the MN performs handover between enhanced nodes, the HKS needs to be contacted to generate HK in both of the previous and the proposed solutions. Thus, the two solutions would perform similarly by introducing the extra RRT to interact with the HKS. When the MN performs handover between ARs within one enhanced node domain, the previous mechanism still introduce one extra RRT for key generation. However, there is no extra RRT involved in the proposed solution, as the MN already has the keying material. The only extra time introduced is the time MN needs to generate the HK using the keying material in its memory. The key generation time can be almost neglected, comparing to the RRT to the HKS. More detailed analysis for handover delay is provided in Appendix D.

It should be also noted that the replay protection is not provided in the mechanism. However, timestamp based replay protection between MN and HKS is possible, by inserting a “timestamp” mobility option to the message. The timestamp can be verified to be valid, if it is in within certain value. The clocks need to be synchronized, if the timestamp based anti-replay method is used. Otherwise, it may result in one more RRT to synchronize the clock.
Chapter 6

6 Secure Fast Handovers in HMIPv6

6.1 Integration of HMIPv6 with Fast Handovers

The concept of "Fast Handover" primarily aims to minimise handover latency. FMIPv6 is introduced to improve the handover latency resulting from the MIPv6 procedures. The operation of FMIPv6 protocol was introduced in section 2.1.2.3. The FMIPv6 protocol enables an MN to quickly detect that it has moved to a new subnet when the MN is still connected to its current subnet. Before the MN establishes the connection with the new AR, the packets still arrive at previous AR and will be redirected to the new AR.

The idea of integrating FMIPv6 and HMIPv6 (F-HMIPv6), is also explained in section 2.1.2.4. The invention of HMIPv6 allows MIPv6 to benefit from not only reduced mobility signalling but also less additional delay element resulting from global updates to HA and all CNs. With the introduction of MAP, the handover latency related to global location updates is considerably reduced, as the MN only needs to update its MAP if the handover is performed within one MAP domain. Therefore, the necessity of integrating HMIPv6 with fast handovers when the handoff is performed locally within one MAP domain is not as appealing as the others. Although, there are some investigations carried out in HMIPv6 standard [6]. In [6], it is specified a method to integrate HMIPv6 with FMIPv6. In this method, MAP is placed above the ARs as an aggregation router, thus, the fast handover negotiating and packets forwarding takes place between MAP and new AR, instead of between PAR and NAR as defined in FMIPv6 standard. The integration of HMIPv6 and fast handovers is illustrated in Figure 6.1. Figure (1) shows the idea of using MAP as the anchor point of initiating and negotiating fast handover process, as specified in [6]. In this case, MAP processes the FBU request from the MN and exchanges messages with the NAR regarding the handovers. Figure (2) shows the concept of basic fast handover procedures proposed in FMIPv6 standard. As opposed to figure (1), PAR is used here as the anchor point for fast handovers. It can be noticed (figure (1) ) that the message exchanges to enable MAP to forward packets to NAR is probably the same as those needed to perform the local location update, thus, it is not wise to involve MAP as the anchor point to achieve fast handovers. Based on the
assumption that ARs be connected for location registration and packet forwarding, the method in figure (2) is a natural way to implement fast handovers in HMIPv6.

![Diagram of FAST HANDOVERS IN HMIPv6](image)

**Figure 6.1 Integration of HMIPv6 and fast handovers**

In the situation where handover is performed between different MAP domains, the fast handover mechanism is more necessary, as the global location update is believed to be time-consuming and can cause noticeable disruptions. It is explained in section 2.1.2.4 the method to enhance HMIPv6 with fast handovers in the scenario of inter-MAP domain handovers. As shown in Figure 2.6 and Figure 2.7, the handover negotiation is performed between previous MAP and new MAP, and the packets are forward from PMAP to NMAP.

### 6.2 Security Considerations

It is discussed in section 6.1 the integration of fast handovers and HMIPv6 in both of the micromobility and macromobility scenarios (defined in Figure 5.1). In either of the two scenarios, there are two main security vulnerabilities to be identified and solved as follows,

- **Secure FBU**

  Insecure FBU can cause security threat, for instance, packets meant for one address could be stolen or redirected to the malicious node. Hence, the PAR needs ensure that the FBU packet arrived from a node that is authentic and legitimately owns the PCoA. Therefore, the access router and MN should use certain mechanism to establish a security association which is used to secure the FBU.

  In the micromobility handover scenario, the FBU/FBA is exchanged between MN and PAR, and in the macromobility handover scenario, they are exchanged between MN and PMAP via
PAR. Therefore, using the handover keys established by the mechanism in chapter 5, the FBU can be secured.

- Secure handover negotiation and context transfer between ARs/MAPs.

Two types of messages are possible to be exchanged between neighbouring ARs/MAPs:

a. HI/Hack messages

The Handover Initiate (HI) and Handover Acknowledgment (HAck) messages are exchanged between ARs/MAPs to negotiate the handover. It is suggested in the FMIP standard [7] that HI/Hack must be protected using end-to-end SAs to offer integrity and data origin authentication.

b. QoS context transfer

In some scenarios, context transfer occurs between neighbouring ARs/MAPs. It is proposed in [11] a combined mobility QoS mechanism based on HMIPv6 (with details in Appendix E). In this mechanism, QoS context transfer is performed between enhanced nodes if it is a handover across enhanced nodes.

To protect the two types of message exchanges, it is important to establish keys between neighbouring ARs/MAPs. This chapter will provide solutions for establishing keys between ARs/MAPs to secure the fast handovers in HMIPv6 networks.

### 6.3 Previous work

Aiming at solving the two main security vulnerabilities explained in section 6.2, some work has been carried out to establish keys to secure FBU or to protect message exchanges between neighbouring ARs/ENs. It is proposed in [82] a method using SEND for providing a shared key from AR to MN to protect the signalling. As discussed in section 5.1, a lot work has been undertaken using CGA related method to establish SA for the purpose of securing FBU. And the mechanism making use of AAA infrastructure proposed in chapter 5 can be also used to establish keys between AR and MN. Hence, one of the major areas where work still needs to be done is to establish SA between neighbouring ARs/ENs.

Relatively less work has been undertaken in establishing SA between ARs/ENs. It is specified in [97] a mechanism to secure packet forwarding using a temporary session key. In intra-MAP handoff, the temporary session key is established between old AR and new AR, while in inter-MAP handoff procedure, the session key is established between old MAP and new MAP. However, this mechanism only focuses on reducing unnecessary overhead introduced by AAA solution in terms of authentication and key distribution, and the integration of mobility and security is not achieved. Since fast handover signalling is not considered to be integrated with the
security procedure, security signalling could have negative impact on MIP protocols, in terms of introducing large handover latency and too much signalling overhead.

In this chapter, I introduce the mechanism to establish keys between neighbouring ARs/ENs to secure the fast handovers in HMIPv6 networks. A trusted third party (either the EN or the AAA server) is involved in the key generation and distribution.

6.4 Description of the Mechanism

6.4.1 Security Association (SA) model

It is assumed that AAA infrastructure exists for the Mobile IP application. And it is assumed that some pre-established trust exists between some of the network elements. The trust model is shown in Figure 6.2. As illustrated in the figure, the visited network is divided into four hierarchies: MN, ARs, enhanced node (EN) and AAA servers in the foreign network. In order to establish SA between neighbouring ARs (PAR-NAR) and between neighbouring ENs (PEN-NEN), the following pre-established SAs are assumed,
- SA exists between enhanced node and the ARs in its domain.

This assumption is the same as described in section 5.2.2. Using the intelligence of the EN, the EN is able to have knowledge about surrounding entities and can manage the ARs in its domain. The establishment of SA between EN and AR is outside the scope of discussion. However, the HKs established between EN and AR using the mechanism in chapter 5 can be used for this
purpose, if MAP does not have EN functionality and is not able to establish SA with ARs within its domain.

- SA exists between AAAF server and the enhanced nodes

It is assumed that AAA infrastructure is used for Mobile IP application. The enhanced node, acting as the mobility agent in mobile IP, is supposed to have part of the functionality of AAA client. It is required in the AAA/MIP application that the mobility agents have a permanent trust relationship with the AAA server within the domain they belong to, such as HA-AAAAH server, MAP-AAAF server, etc. Hence, AAA messages that includes keys/keying materials can be carried in a secured link.

SAs also exist between MN and the ARs to secure FBU. They can be established using the mechanism explained in chapter 5.

6.4.2 Handover between ARs within One Enhanced Node Domain

The predictive fast handover is assumed here. In the predictive mode, the fast handover is initiated in advance so that an MN is able to send an FBU when it is still attached to the PAR, which then enables forwarding traffic even before the MN attaches to the NAR. There are two types of methods to initiate the handover: network initiated handover and MN initiated handover. In a MN initiated handover, the MN sends a Router Solicitation for Proxy Advertisement (RtSolPr.) message to PAR to prompt ARs for Proxy Router Advertisements (PrRtAdv.). In response, the PAR sends PrRtAdv. message back to the MN, providing the link-layer address, IP address, and subnet prefixes of neighbouring routers. In a network initiated handover, the handover control resides in the network. In such scenario, the PAR sends an unsolicited PrRtAdv containing information of the NAR. The unsolicited PrRtAdv allows the network to inform the MN about geographically adjacent AR without the MN requesting that information. It reduces the amount of wireless traffic required for the MN to obtain information about neighbouring AR. Upon receiving the PrRtAdv. message, the MN processes it to configure the new CoA. The two different modes of handover initiation are shown in Figure 6.3.

In both of the MN initiated and the network initiated handover, the MN sends a FBU to the PAR after the PrRtAdv. message is processed. The signalling of the mechanism is shown in Figure 6.3. The messages in italics are the security related signalling to establish fast handover key between neighbouring ARs (PAR and NAR). More details are explained as follows,
Chapter 6. Secure fast handovers in HMIPv6

Figure 6.3 Signalling for handover within one enhanced node domain

1. FBU

Fast BU message is sent by the MN instructing PAR to redirect traffic to the NAR. This can be achieved by creating a binding between the previous CoA (PCoA) and new CoA (NCoA). The format of FBU message is identical to the standard MIPv6 BU message, however, the FBU message is with different flag values and mobility options.

Figure 6.4 FBU message format [7]

It is proposed here two one-bit flags using the reserved field: “T” flag and “S” flag as highlighted in red in Figure 6.4. “T” flag indicates the fast handover type. With “T” value set to 0, the message is the FBU message for handover within one EN domain. With “T” value set to 1, the...
message is for fast handover between ENs. Please be noted that the message might contain different mobility options for handover within/across EN, although the message field is the same as shown in Figure 6.4. “S” flag indicates whether security mechanism will be triggered or not. If “S” flag value is set to 0, the normal fast handover procedure will be carried out, without the security messages (FKH Req. and FHK Resp.) being involved. If “S” flag value is set to 1, the PAR will need to initiate a fast handover key request message (FKH Req.) in order to obtain a fast handover key to be shared with the NAR. With “S” value equal to 0, the mobility option in the FBU message only includes these options suggested by the FMIPv6 specification, such as alternative CoA option. With “S” value set to 1, more mobility options need to be included, apart from the compulsory ones defined in FMIPv6. The mandatory ones are:

- NAR’s IP address mobility option

IP address/prefix option defined in Mobile IPv6 fast handovers specification [7] can be used to carry the NAR’s IP address. With “option-code” value set to 3, the IP address option carries NAR’s IP address.

- MN identifier mobility option

The MN identifier mobility option is used to carry the MN’s NAI. The MN identifier mobility option is defined in RFC 4283 [89], thus, there is no need to introduce a new mobility option here.

2. FHK Req.

![Figure 6.5 Fast handover key request message](image)

The PAR sends a FHK Req. message to the enhanced node. It basically instructs the enhanced node to generate a FHK to be used between the PAR and the NAR. The FHK Req. message uses MH type value “TBA1”. The NCoA is included this message, as the keying material that EN needs to generate FHK. Please be noted that the NCoA here is the CoA that the MN proposes to use in the new link. However, the NAR can deny using the NCoA and proposes another NCoA which is mandatory for MN to use in the new link. The format of message data field in the MH is shown in Figure 6.5. The options filed can carry different mobility options as required. The mandatory options are the MN identifier mobility option and the NAR’s IP address mobility.
option, as explained in last section. If the integrity protection is required for the message, the MAC mobility option can be included in the "options" field.

The FHK is derived in a similar method as explained in section 5.3.2.2,

\[ FHK = gprf^+ \text{(key, string)}; \]

where, key is a seed to generate the FHK which can be refreshed by the EN periodically; string = \( N_{EN} | ID_{MN} | PCoA | NCoA \) “Fast Handover Key”; \( Y = 0\times0000 \). \( N_{EN} \) is a nonce generated by the EN for FHK. \( ID_{MN} \) is the MN's NAI. The EN can obtain the PCoA by checking its binding cache. The NCoA, which is the NCoA MN proposes to use, is included in the FHK Req. message.

3. and 4. FHK Resp.

The enhanced node generates the FHK, and sends a fast handover key response (FHK Resp.) message to the PAR, in response to the FHK Resp. message. The enhanced node also sends an unsolicited FHK Resp. message to NAR. The FHK Req. message uses MH type value 'TBA2'. As SA is assumed to exist between EN and all ARs within its domain, the FHK Resp. message can be secured. The format of message data field in the MH is shown in Figure 6.6.

![Figure 6.6 Fast handover key response message](image)

![Figure 6.7 FHK mobility option](image)

The message ID is to match the FHK Resp. message with corresponding request. And the result of key generation is indicated in "result code" field. Different values of the result code indicate the status of the request: '0' indicates success, while other values may be assigned to different reasons of failure. The lifetime (in seconds) of FHK is carried in "lifetime" field. "Reserved" field
is set to 0 and ignored upon reception. The four-byte “SPI” carries the SPI to index the FHK. The “options” field can carry different mobility options as required. The mandatory option that must be carried in the FHK Resp. message is: FHK mobility option (as shown in Figure 6.7), which includes the FHK. Similarly to the FHK Req. message, MAC mobility option can be included in “options” field to provide message authentication.

Upon receiving the FHK Resp. message from the EN, PAR and NAR obtain the FHK and corresponding SPI. The PAR then sends handover initiate (HI) message to the NAR regarding the MN’s handover, before creating a binding between PCoA and NCoA.

5. and 6. HI/HAck.

The PAR exchanges HI and handover acknowledgement (HAck) messages with NAR. The main purpose of HI and HAck messages is to determine whether the NCoA is valid. If the NCoA is already in use in NAR’s link, the NCoA is not valid and NAR will propose another NCoA, which will be transmitted to PAR in the HAck message.

7. FBA

In response to the FBU, the PAR sends a FBA message to MN. If there is a NCoA assigned by the NAR, the MN will be notified in the FBA message. And the MN must use the assigned NCoA upon its attachment to the NAR.

8. UNA

Unsolicited Neighbour Advertisement (UNA) message is sent by the MN to the NAR, as soon as the MN establishes connectivity on the new link. It is basically to instruct the NAR to forward the arriving or buffered packets to the MN.

### 6.4.3 Handover between Enhanced Nodes

To integrate HMIPv6 with fast handovers, the handover between enhanced node domains is crucial. As the global location update could result in noticeable handover disruption and packet loss. The procedure is explained in section 2.1.2.4, and the signalling is illustrated in Figure 2.7. The predictive mode is considered in this section, which means the fast handover is triggered in advance so that the FBA message is received on the previous enhanced node’s link.

The information for a potential handover is exchanged between MN and PAR either through RtSolPr./PrRtAdv. messages in a MN initiated handover or through unsolicited PrRtAdv. message in a network initiated handover. Using the information contained in the router advertisement message, the MN obtains the new LCoA to be used in the NAR’s link and the new RCoA to be
used in the NEN’s domain. In the router advertisement, MAP option is included. This RCoA is constructed by combining the MN’s interface identifier and the subnet prefix received in the MAP option.

The signalling details shown in Figure 6.8, are explained as follows,

1. and 2. FBU

The MN initiates a FBU to the previous EN through previous AR. This is to instruct PEN to buffer the packets to MN with previous CoA as the destination address. The MN’s new LCoA and new RCoA are also included in FBU, so that the PEN can check the validity of new addresses with New EN in the following message exchanges.

With “T” and “S” flag values set to 1 (as shown in Figure 6.4), the FBU message is for handover between ENs and requires key to be established between PEN and NEN. Apart from the regular mobility options for fast handover, the other mandatory mobility options include:

- MN identifier mobility option, as explained in section 6.4.2
- NEN’s IP address mobility option

IP address/prefix option defined in Mobile IPv6 fast handovers specification [7] can be used to carry the NEN’s IP address. It is proposed that the value of “option-code” is set to 5, thus, the “IP address” field carries NEN’s IP address.

Please be noted that there are two types of FBU message: MN→PAR and PAR→PEN. And the mobility options in the messages may vary. For instance, the IP address option which carries MN’s previous LCoA needs to be included in the FBU from PAR to PEN.

3. AAA Req.

Upon receiving the FBU message, the previous EN realizes that the fast handover procedure has been triggered and the fast handover key is required if the “S” flag in FBU is set to 1 (as explained in section 6.4.2). To establish the fast handover key with new EN, the previous EN should consult AAAF server. The previous EN initiates the AAA Req. message to the AAAF server, requesting the AAAF server to generate the fast handover key. The “DIAMETER-FHK-Request” command is proposed here, similar to the “DIAMETER-HK-Request” command defined in section 5.3.3.3. In the DIAMETER-FHK-Request command, it includes the information that the AAAF server needs to generate the fast handover key. In this command, the following AVPs must be included to carry the information to AAAF server,

- Mobile-Node-Identifier AVP
This AVP (AVP Code 506) is defined in section 5.6 of RFC 5779 [98]. This AVP contains the mobile node identifier in the NAI format.

- MIP-CoAs AVP

It is a grouped AVP, which contains MIP-Careof-Address AVPs (AVP Code 487) defined in section 6.7 of RFC 5778 [38]. It carries the MN's previous RCoA and new RCoA.

- EN-IP-Address AVP

It is an address type AVP proposed here to carry the new EN's IP address. It is similar to "Host-IP-Address" AVP defined in RFC 3588 [31].

Once the AAA Req. message is received, the AAAF server should generate a fast handover key. The FHK is derived in a similar method as explained in section 5.3.2.2:

\[ FHK = \text{gprf}^+ (\text{key}, \text{string}); \]

where, key is a seed to generate the FHK which can be refreshed by the EN periodically; string = \( N_{AAA} | ID_{MN} | \text{previous RCoA} | \text{new RCoA} | \text{"Fast Handover Key"}; Y = 0x0000 \). \( N_{AAA} \) is a nonce generated by the AAAF server. \( ID_{MN} \) is the MN's NAI.

4. and 5. AAA Resp.

The AAAF server generates the fast handover key, and sends an AAA response message to the previous EN. The AAAF server also sends an unsolicited AAA message to the new EN. In the AAA response message, "DIAMETER-FHK-Response" command is proposed here to carry the FHK and related information to both of the previous EN and new EN. The command is similar to the "DIAMETER-HK-Response" command defined in section 5.3.3.3. The following AVPs must exist in the command:

- Result-Code AVP

Result-Code AVP (AVP code 268) is defined in RFC 3588 [31] and can be used to indicate the result of FHK generation. In this AVP, one value is assigned to indicate "success", and other value is assigned to suggest reasons of "failure".

- Mobile-Node-Identifier AVP

This AVP (AVP Code 506) is defined in section 5.6 of RFC 5779 [98]. This AVP contains the mobile node identifier in the NAI format.

- MIP-Session-Key AVP
MIP-Session-Key AVP (AVP code 343) defined in section 9.7 of RFC 4004 [36] can be used to carry the fast handover key. The AAA response message or the MIP-Session-Key AVP can be secured using SA existed between the AAAF server and the EN.

- MIP-sessionkey-SPI AVP

The AVP is proposed here to carry the SPI of the fast handover key. It is similar to the "MIP-FA-to-MN-SPI" AVP defined in RFC 4004 [36].

- MIP-MSA-Lifetime AVP

MIP-MSA-Lifetime AVP (AVP code 367) defined in section 9.13 of RFC 4004 [36] can be used to indicate the period of time (in seconds) for which the FHK is valid.

![Figure 6.8 Signalling for handover between enhanced nodes](image)

6. and 7. HI/HAck

The previous EN and new EN exchange information through HI/HAck messages to negotiate with each other regarding the MN’s handover. The HI message contains the new LCoA and new RCoA of the MN. The new EN needs to validate the new RCoA and new LCoA by checking
whether it has been used or not. If the validation fails, the new EN proposes another LCoA to be used by the MN which will be transmitted to previous EN in HAck message. If the validation is successful, the new EN creates a temporary binding between the new LCoA and the new RCoA. The new EN also provides the status of the handover request in the HAck message to the previous EN. The previous EN then creates a binding between MN's previous RCoA and new RCoA.

8. and 9. FBA

Having received HAck message, the previous EN sends a FBA message to MN in response to FBU. The fast handover registration is completed by now. Afterwards, the packets addressed to MN's previous location can be tunnelled from the previous EN to the new EN.

10. and 11. UNA

UNA message is sent by the MN to NAR and new EN, as soon as the MN establishes connectivity on the new link. It is basically to instruct the new EN to forward the arriving or buffered packets to the MN.

6.5 Analytical Models

The following parameters are defined in order to obtain the signalling cost,

- \( i \): number of ARs an MN crossed between two consecutive packet arrivals.
- \( \alpha(i) \): probability that an MN crossed \( i \) ARs between two packet arrivals [99].
- \( N \): the number of ARs in each enhanced node domain is assumed to be the same and is equal to \( N \). It is assumed that \( N=4 \).
- \( k \): number of ARs crossed between the last packet arrival and the last enhanced node crossing. It is assumed that \( k=3 \).

6.5.1 Network Model

It is shown in Figure 6.9 the network model. As illustrated in the figure, there are four ARs within each enhanced node domain, thus, \( N=4 \). The fast handover can be performed between ARs within one enhanced node domain, and can also be performed between enhanced nodes. As explained in section 6.4.3, the AAAF server is involved in the handover between enhanced nodes, for the purpose of FHK generation.
6.5.2 Signalling Cost for Mobility Location Update

FHMIPv6-enabled MN should be able to operate in the HMIPv6 domain with fast handovers in order to address the issues of large handover latency and packet loss. Therefore, the location update can be divided into two parts: HMIPv6 related registration and fast handover related registration, as shown in Figure 6.10. In the HMIPv6 related registration, the MN updates the enhanced node and also update the HA/CN when the MN changes the enhanced node domain. In the fast handover related registration, the previous AR/EN is temporarily registered with the new AR/EN, in the handover within one enhanced node and across enhanced nodes, respectively.

The HMIPv6 registration cost is the sum of location update cost to EN, HA and CNs. Location updates cost for MN to update EN/HA/CN are $LU_{EN}$, $LU_{HA}$ and $LU_{CN}$. And they are illustrated in Figure 6.10 and can be expressed as follows,
Chapter 6. Secure fast handovers in HMIPv6

\[ LU_{\text{EN}} = 2P_{\text{ar}} + P_{\text{en}} + H_{\text{m-ar-en}}^\text{en} + H_{\text{ar-en}}^\text{en} \quad \text{Eq. 6-1} \]

\[ LU_{\text{HA}} = 2P_{\text{ar}} + 2P_{\text{en}} + P_{\text{ha}} + H_{\text{m-ar-en}}^\text{en} + H_{\text{ha-en}}^\text{en} + H_{\text{en-ha}}^\text{en} \quad \text{Eq. 6-2} \]

\[ LU_{\text{CN}} = 2P_{\text{ar}} + 2P_{\text{en}} + n \cdot P_{\text{en}} + H_{\text{m-ar-en}}^\text{en} + n \cdot H_{\text{en-cn}}^\text{en} \quad \text{Eq. 6-3} \]

where, \( n \) is the number of CNs communicating with MN when the handover takes place. \( H_{a-b}^X \) is the signalling cost for location update message between entity a and b, to entity X. For instance, \( H_{\text{m-ar-en}}^\text{en} \) is the signalling cost for location update message (BU/BA messages) to EN, between MN and AR. \( P_{\text{en}} \) is the processing cost for the location update message at entity a.

The fast handover registration cost is composed of location update cost for fast handover between ARs (\( LU_{\text{FH,AR}} \)) and location update cost for fast handover between enhanced nodes (\( LU_{\text{FH,EN}} \)). And they are illustrated in Figure 6.10 and can be expressed as follows,

\[ LU_{\text{FH,AR}} = 3P_{\text{ar}} + F_{\text{mn-par}} + F_{\text{par-nar}} \quad \text{Eq. 6-4} \]

\[ LU_{\text{FH,EN}} = 2P_{\text{ar}} + 3P_{\text{en}} + F_{\text{en-par}} + F_{\text{par-pen}} + F_{\text{pen-enn}} \quad \text{Eq. 6-5} \]

where, \( F_{a-b} \) is the signalling cost for fast handover location update message between entity a and b. For example, \( F_{\text{par-nar}} \) is signalling cost for messages between PAR and NAR (HI/HAck messages). Please be noted that the UNA message is not considered as location update message here, as it is to instruct the new AR/EN to forward packets to the MN.

It can be easily known that MN handovers across enhanced node domains \( \left\lceil \frac{i+k}{N} \right\rceil \) times, thus, it updates HA/CN/previous enhanced node \( \left\lceil \frac{i+k}{N} \right\rceil \) times. And MN handovers across ARs within one enhanced node domain \( \left( i - \left\lceil \frac{i+k}{N} \right\rceil \right) \) times, thus, the MN updates enhanced node/previous AR \( \left( i - \left\lceil \frac{i+k}{N} \right\rceil \right) \) times.

Let \( C_{\text{LU}} \) denote the total signalling cost for all location updates, thus,

\[ C_{\text{LU}} = \sum_{i=0}^{\infty} \left[ \left\lceil \frac{i+k}{N} \right\rceil - \left\lceil \frac{i+k}{N} \right\rceil \right] \cdot \alpha(i) \cdot (LU_{\text{FH,EN}} + LU_{\text{EN}} + LU_{\text{HA}} + LU_{\text{CN}}) \]

\[ + \sum_{i=0}^{\infty} \left( i - \left\lceil \frac{i+k}{N} \right\rceil \right) \cdot \alpha(i) \cdot (LU_{\text{FH,EN}} + LU_{\text{EN}}) \quad \text{Eq. 6-6} \]

where, \( \alpha(i) \) denotes the probability that MN moves across \( i \) ARs between two consecutive packet arrivals. Substituting Eq. 6-1, Eq. 6-5 into Eq. 6-6, \( C_{\text{LU}} \) can be then expressed as,
Chapter 6. Secure fast handovers in HMIPv6

\[ C_{ij} = \sum_{i=0}^{\delta} \frac{a(i)}{N} \cdot \left( \frac{2P_{ar} + 3P_{en} + F_{e-s}-p+iF_{p-s-n} + F_{p-w-n}}{2P_{ar} + 2P_{en} + nF_{e-s}-p+iF_{p-s-n} + F_{p-w-n}} \right) \]

\[ + \sum_{i=0}^{\delta} \left( \frac{a(i)}{N} \cdot \left( 3P_{ar} + F_{e-s}-p+iF_{p-s-n} \right) \right) \]

The transmission cost is assumed to be proportional to the distance between the source and destination entities. And \( \delta \) denotes the unit transmission cost in a wired link. It is assumed that the unit transmission cost is the cost for local BU to enhanced node in HMIPv6. The following parameters are also defined to calculate the signalling cost:

- \( \omega \): It is assumed that the transmission cost over a wireless link is \( \omega \) times of the cost over a wired link.

- \( \delta_X^{a} \): transmission cost coefficient for mobility signalling message X in HMIPv6 to/from entity a.

It is defined as: \( \delta_X^a = \frac{\text{bandwidth consumption for mobility signalling message X in a wired link}}{\text{bandwidth consumption for local BU in a wired link}}. \)

The corresponding coefficients are listed as follows,

a. \( \delta_{EN}^{BA} \): transmission cost coefficient for local BA from enhanced node

b. \( \delta_{BU}^{HA} \): transmission cost coefficient for BU to HA

c. \( \delta_{BU}^{BA} \): transmission cost coefficient for BA from HA

d. \( \delta_{BU}^{CN} \): transmission cost coefficient for BU to CN

e. \( \delta_{BU}^{CN} \): transmission cost coefficient for BU from CN

- \( \theta_X^{AR/EN} \): transmission cost coefficient for mobility message X in fast handover between ARs/ENs. The corresponding coefficients are listed as follows,

a. \( \theta_{FBU}^{AR} \): transmission cost coefficient for FBU message in fast handover between ARs

b. \( \theta_{FBA}^{AR} \): transmission cost coefficient for FBA message in fast handover between ARs

c. \( \theta_{HI}^{AR} \): transmission cost coefficient for HI message in fast handover between ARs

d. \( \theta_{Hack}^{AR} \): transmission cost coefficient for Hack message in fast handover between ARs

e. \( \theta_{FBU}^{EN} \): transmission cost coefficient for FBU message in fast handover between enhanced nodes

f. \( \theta_{FBA}^{EN} \): transmission cost coefficient for FBA message in fast handover between enhanced nodes

g. \( \theta_{HI}^{EN} \): transmission cost coefficient for HI message in fast handover between enhanced nodes

145
h. $\theta_{HAck}^{EN}$: transmission cost coefficient for HAck message in fast handover between enhanced nodes

- $D_{a-b}$: distance (number of hops) between entity $a$ and $b$. And $D_{a-b} = D_{b-a}$. For instance, $D_{AR-EN}$ is the number of hops between AR and enhanced node, $D_{AR-AR}$ is the number of hops between neighbouring ARs (PAR and NAR).

Thus, $C_{LU}$ can be expressed as follows,

$$
C_{LU} = \sum_{i=0}^{n} \left\{ \frac{i+k}{N} \cdot \alpha(i) \cdot \left[ \frac{(8P_{ar} + 8P_{en} + P_{ha} + n \cdot P_{ca})}{N} \cdot \left( H_{m-ar} + H_{m-en} + n \cdot H_{ca} \cdot \delta \cdot (1 + S_{EN}) \right) 
+ \left( \omega \cdot D_{m-ar} + D_{m-en} + n \cdot D_{ca} + \delta \cdot (\delta_{HA}^{LH} + \delta_{HA}^{R}) \right) + \omega \cdot D_{m-ar} + D_{m-en} + n \cdot D_{ca} + \delta \cdot (\delta_{CN}^{LH} + \delta_{CN}^{R}) \right] \right\} + \sum_{i=0}^{n} \left( i - \left\lfloor \frac{i+k}{N} \right\rfloor \right) \cdot \alpha(i) \cdot \left[ \frac{(5P_{ar} + P_{en})}{N} \cdot \left( 1 + \delta_{EN} \cdot \delta \cdot (\theta_{FBU}^{EN} + \theta_{FRA}^{EN}) + D_{en-ca} \cdot \delta \cdot (\theta_{H}^{EN} + \theta_{H}^{EN}) \right) \right] \right\}
$$

(1) handover within one EN domain
Figure 6.10 Signalling cost for location update and security. (1) fast handover between ARs within one enhanced node domain; (2) fast handover between enhanced nodes

6.5.3 Security Signalling Cost

The security mechanism introduces extra signalling messages, as shown in Figure 6.3 and Figure 6.8. The extra signalling cost is calculated in the following sections.

6.5.3.1 Handover within One Enhanced Node Domain

As shown in Figure 6.3, the security mechanism introduces signalling messages between PAR and EN, NAR and EN. And with security mechanism enabled, the fast handover location update messages need to carry more information in the mobility options, which results in more signalling cost. Let $SE_{AR}$ denote security signalling cost for handover between ARs within one EN domain. Then, $SE_{AR}$ can be calculated as,
Chapter 6. Secure fast handovers in HMIPv6

\[ SE_{en} = 3P_{ar} + 3S_{ar} + S_{en} + S_{mn-par} + S_{par-nar} + S_{par-en} + S_{nar-en} \]
\[ = 3P_{ar} + 3S_{ar} + S_{en} + \omega \cdot D_{mn-ar} \cdot e_{SBU} \cdot \delta + \omega \cdot D_{mn-ar} \cdot e_{SFBA} \cdot \delta \]
\[ + D_{ar-en} \cdot e_{SHI} \cdot \delta + D_{ar-en} \cdot e_{SHACK} \cdot \delta + D_{en-en} \cdot e_{1} \cdot \delta + D_{en-en} \cdot e_{2} \cdot \delta + D_{en-en} \cdot e_{3} \cdot \delta \]

Eq. 6-9

where, \( S_{ar} \) and \( S_{en} \) are the processing cost for security message at AR and EN. \( S_{mn-par} \), \( S_{par-nar} \), \( S_{par-en} \) and \( S_{nar-en} \) are the security signalling cost between MN and PAR (FBU/FBA), PAR and NAR (HI/HACK), PAR and EN (FHK Req./Resp.), NAR and EN (FHK Resp.), as shown in (1) Figure 6.10. \( \epsilon_{1}, \epsilon_{2} \) and \( \epsilon_{3} \) are transmission cost coefficients for corresponding security signalling messages: FHK Req. sent from PAR to EN, FHK Resp. sent from EN to PAR, FHK Resp. sent from EN to NAR. It is defined as:

\[ \epsilon_{1,2,3} = \frac{\text{bandwidth consumption for certain security signalling message in a wired link}}{\text{bandwidth consumption for local BU in a wired link}}. \]

And \( \epsilon_{SBU}, \epsilon_{SHI} \) and \( \epsilon_{SHACK} \) are transmission cost coefficients for FBU, FBA, HI and HACK messages with security mechanism enabled.

### 6.5.3.2 Handover between Enhanced Node Domains

As shown in Figure 6.10, the security mechanism introduces signalling messages between PEN and AAAF server, NEN and AAAF server. Let \( SE_{EN} \) denote security signalling cost for handover between enhanced nodes. Then, \( SE_{EN} \) can be calculated as,

\[ SE_{EN} = 2P_{ar} + 3P_{en} + 3S_{en} + S_{aaa} + S_{mn-par} + S_{par-pen} + S_{pen-nen} + S_{pen-aaa} + S_{aaa} \]
\[ = 2P_{ar} + 3P_{en} + 3S_{en} + S_{aaa} + \omega \cdot D_{mn-ar} \cdot e_{1}^{SBU} \cdot \delta + \omega \cdot D_{mn-ar} \cdot e_{1}^{SFBA} \cdot \delta \]
\[ + D_{ar-en} \cdot e_{1}^{SHI} \cdot \delta + D_{ar-en} \cdot e_{1}^{SHACK} \cdot \delta + D_{en-en} \cdot e_{2} \cdot \delta + D_{en-en} \cdot e_{3} \cdot \delta \]

Eq. 6-10

where, \( S_{en} \) and \( S_{aaa} \) are the processing cost for security message at EN and AAAF server. \( S_{mn-par}, S_{par-pen}, S_{pen-nen}, S_{pen-aaa} \) and \( S_{aaa} \) are the security signalling cost between MN and PAR (FBU/FBA), PAR and PEN (FBU/FBA), PEN and NEN (HI/HACK), PEN and AAAF server (AAA Req./Resp.), NEN and AAAF server (AAA message), as shown in (2) Figure 6.10. \( \epsilon_{1}, \epsilon_{2} \) and \( \epsilon_{3} \) are transmission cost coefficient for certain security signalling message: AAA Req. sent from PEN to AAAF server, AAA Resp. sent from AAAF server to PEN, AAA message sent from AAAF server to NEN. And \( \epsilon_{1}^{SBU}, \epsilon_{1}^{SFBA}, \epsilon_{1}^{SHI} \) and \( \epsilon_{1}^{SHACK} \) are transmission cost coefficients for FBU (MN-PAR), FBA (PAR-MN), FBU (PAR-PEN), FBA (PEN-PAR), HI and HACK messages with security mechanism enabled, respectively.

148
Chapter 6. Secure fast handovers in HMIPv6

Since MN performs handovers between enhanced nodes \( \left[ \frac{i+k}{N} \right] \) times and handovers between ARs within one EN domain \( \left( i - \left[ \frac{i+k}{N} \right] \right) \) times, the total security signalling cost \( S \) can be expressed as:

\[
S = \sum_{i=0}^{\infty} \alpha(i) \cdot \left\{ \left( i - \left[ \frac{i+k}{N} \right] \right) \cdot SE_{AR} + \left\lfloor \frac{i+k}{N} \right\rfloor \cdot SE_{EN} \right\} \quad \text{Eq. 6-11}
\]

Substituting Eq. 6-9 and Eq. 6-10 into Eq. 6-11, the total security signalling cost \( S \) can be derived.

The values of parameters are listed in Table IV of Appendix C.

In order to derive \( \alpha(i) \), the following assumptions are made:

- \( t_c \): time between two consecutive packet arrivals. And it is assumed that mean value of \( t_c \) is \( E(t_c) = 1/\lambda_c \). And \( t_c \) is independent and identically distributed (iid). \( t_c \) follows exponential or Erlang distribution. \( f_c(t) \) is probability density function of \( t_c \). \( f_c^*(s) \) is laplace transform of \( f_c(t) \).

- \( t_i \): AR i residence time. And it is assumed that mean value of \( t_i \) is \( E(t_i) = 1/\lambda_m \). And \( t_i \) is independent and identically distributed (iid). \( t_i \) follows Gamma distribution. \( f_m(t) \) is probability density function of \( t_i \). \( f_m^*(s) \) is laplace transform of \( f_m(t) \).

If \( t_c \) follows exponential distribution with \( \lambda_c \), then the probability density function and its laplace transform can be expressed as:

\[
f_c(t) = \lambda_c \cdot e^{-\lambda_c t} \quad \text{Eq. 6-12}
\]

\[
f_c^*(s) = \frac{s}{s + \lambda_c} \quad \text{Eq. 6-13}
\]

If \( t_c \) follows Gamma distribution, then the probability density function and its laplace transform can be expressed as:

\[
f_c(t) = t^{k-1} \cdot \frac{e^{-\theta t}}{\theta^k \Gamma(k)} = \frac{\alpha^k t^{\gamma-1}}{\Gamma(\gamma)} \cdot e^{-\alpha t} \quad \text{for } t > 0 \text{ and } k, \theta > 0 \quad \text{Eq. 6-14}
\]

\[
f_c^*(s) = \left( \frac{1}{s+\theta} \right)^k = \left( \frac{\alpha}{s+\alpha} \right)^\gamma \quad \text{Eq. 6-15}
\]

where, \( \gamma = k \) and \( \alpha = 1/\theta \). When \( k = 1 \), it becomes exponential distribution. If \( k \) is large enough, it is asymptotically normal around \( 1/\lambda_c \). When \( \gamma (k) \) is an integer (\( k=m \)), Gamma distribution becomes an Erlang distribution, thus, the probability density function and its laplace transform can be expressed as:
Chapter 6. Secure fast handovers in HMIPv6

\[ f_c(t) = t^{m-1} \cdot \frac{e^{-\theta t}}{\Gamma(m)} = \frac{\alpha^t t^{m-1}}{\Gamma(m)} \cdot e^{-\alpha t} \quad \text{Eq. 6-16} \]

where, \( \Gamma(m) = (m-1)! \):

\[ f_c^*(s) = \left( \frac{1}{\theta s + 1} \right)^m = \left( \frac{s}{s + \alpha} \right)^m \quad \text{Eq. 6-17} \]

where, \( \alpha = m \lambda_c \).

\( t_i \) follows Gamma distribution, thus, the probability density function and its laplace transform can be expressed as:

\[ f_m(t) = t^{k-1} \cdot \frac{e^{-\theta t}}{\theta^k \Gamma(k)} = \frac{\alpha^t t^{k-1}}{\Gamma(k)} \cdot e^{-\alpha t} \quad \text{Eq. 6-18} \]

\[ f_m^*(s) = \left( \frac{1}{\theta s + 1} \right)^k = \left( \frac{s}{s + \alpha} \right)^k \quad \text{Eq. 6-19} \]

where, \( \alpha = \gamma \lambda_m \).

(1) If \( t_i \) follows Gamma distribution with varying \( \gamma \) and \( \lambda_m \), \( t_c \) follows Exponential distribution with \( \lambda_c \), \( \alpha(i) \) is derived as [61] [99]:

\[ \alpha(i) = \begin{cases} 1 - \frac{1 - f_m^*(\lambda_c)}{\rho} & \text{i=0} \\ \frac{1}{\rho} \left[ 1 - f_m^*(\lambda_c) \right]^i \left[ f_m^*(\lambda_c) \right]^{-1} & \text{i>0} \end{cases} \quad \text{Eq. 6-20} \]

where \( \rho = \lambda_c / \lambda_m \).

(2) If \( t_i \) follows Gamma distribution with varying \( \gamma \) and \( \lambda_m \), \( t_c \) follows Erlang distribution with \( m=2 \) and \( \lambda_c \), \( \alpha(i) \) is derived as [99]:

\[ \alpha(i) = \begin{cases} \frac{(-1)^{m-i}(m \lambda_c)^n}{(m-1)!} \cdot g_0^{(m-i)}(m \lambda_c) & \text{i=0} \\ \frac{(-1)^{m-i}(m \lambda_c)^n}{(m-1)!} \cdot g_0^{(m-i)}(m \lambda_c) & \text{i>0} \end{cases} \quad \text{Eq. 6-21} \]
where, \( g_{0}(s) = \frac{s - \lambda_{m}}{s^{2}} [1 - f_{m}^{(2)}(s)] \), \( g_{i}(s) = \frac{\lambda_{m}}{s^{3}} [1 - f_{m}^{(2)}(s)]^{i} \) and \( x^{(r)}(t) \) denotes the \( r^{th} \) derivative of \( x(t) \). It is assumed that \( m=2 \), therefore, \( g_{0}^{(0)}(s) \) and \( g_{1}^{(0)}(s) \) needs to be derived in order to obtain \( \alpha(t) \).

\[ \alpha(t) = \left\{ \begin{array}{ll}
1 - \frac{\lambda_{m}}{\lambda_{c}} \left( \frac{\gamma \lambda_{m}}{2 \lambda_{c} + \gamma \lambda_{m}} \right)^{i} \left( \frac{\lambda_{m}}{2 \lambda_{c} + \gamma \lambda_{m}} \right) & \text{if } i=0 \\
-\lambda_{m} \left[ h_{i}^{(0)}(2 \lambda_{c}) - 2 h_{i}^{(0)}(2 \lambda_{c} + h_{m}^{(0)}(2 \lambda_{c}) \right] + \frac{\lambda_{m}}{\lambda_{c}} \left[ h_{i-1}^{(0)}(2 \lambda_{c}) - 2 h_{i-1}^{(0)}(2 \lambda_{c} + h_{m}^{(0)}(2 \lambda_{c}) \right] & \text{if } i>0
\end{array} \right. \]

Eq. 6-22

where, \( h_{i}^{(0)}(s) = \left[ f_{m}^{(i)}(s) \right]^{i} \) and \( h_{i}^{(0)}(s) = i \left[ f_{m}^{(i)}(s) \right]^{i-1} \cdot f_{m}^{(i)}(s) = -\frac{i}{\lambda_{m}} \left( \frac{\gamma \lambda_{m}}{s + \gamma \lambda_{m}} \right)^{i+1} \).

### 6.6 Simulation Results

Figure 6.11 Probability vs. number of ARs crossed between two consecutive packet arrivals, \( t_{c} \) follows exponential distribution with \( \lambda_{c}=3 \), and \( t_{m} \) follows Gamma distribution with varying \( \gamma \) and \( \lambda_{m}=30 \). (1) \( \gamma=0.1 \); (2) \( \gamma=0.5 \); (3) \( \gamma=1 \); (4) \( \gamma=10 \).

Figure 6.11 shows probability distribution of the number of ARs crossed between two consecutive packet arrivals, indicating the impact of variance on \( T_{m} \). \( T_{c} \) is the time between two
consecutive packet arrivals, and $T_m$ is AR residence time. It is assumed that $T_c$ follows exponential distribution with $\lambda_c=3$, and $T_m$ follows Gamma distribution with varying $\gamma$ and $\lambda_m=30$. Figure (1), (2), (3) and (4) shows the results with different $\gamma$: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$ and (4) $\gamma=10$. Larger variance of the AR residence time indicates the probability that an MN remains in AR domain for a shorter time. In other words, MN is with higher mobility rate. Therefore, if AR residence time is with a larger variance, a higher number of AR crossed two consecutive packet arrivals occupies a larger amount of the overall number of AR crossed, compared to the AR residence time with smaller variance. For example, the probability of MN crossing two ARs between two consecutive packet arrivals is the highest when $\gamma=10$ and is the lowest when $\gamma=0.1$.

![Figure 6.12 Signalling cost v.s number of ARs crossed between two consecutive packet arrivals.](image)

Figure 6.12 shows the impact of number of ARs crossed between two consecutive packet arrivals on signalling cost (Location update cost in F-HMIP shown in black dotted line and total signalling cost with security mechanism enabled shown in red dotted line). The unit signalling cost is the cost for transmitting a local BU to EN, as defined in section 6.5.2. $T_c$ is assumed to follow exponential distribution and $T_m$ follows Gamma distribution, which is proved to be effective in [99]. Please be noted that the signalling cost is weighed by probability. For example, if the MN moves across 5 ARs, the signalling cost is weighed by the probability that MN crosses 5 ARs between two consecutive packet arrivals. $T_c$ follows exponential distribution with $\lambda_c=3$, and $T_m$ follows Gamma distribution with varying $\gamma$ and $\lambda_m=30$. Figure (1), (2), (3) and (4) shows the results with different $\gamma$: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$ and (4) $\gamma=10$. Larger variance of the AR residence time indicates the probability that an MN remains in AR domain for a shorter time. In other words, MN is with higher mobility rate. Therefore, if AR residence time is with a larger variance, a higher number of AR crossed two consecutive packet arrivals occupies a larger amount of the overall number of AR crossed, compared to the AR residence time with smaller variance. For example, the probability of MN crossing two ARs between two consecutive packet arrivals is the highest when $\gamma=10$ and is the lowest when $\gamma=0.1$. 

![Figure 6.12 Signalling cost v.s number of ARs crossed between two consecutive packet arrivals.](image)
and Tm follows Gamma distribution with varying $\gamma$: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$; (4) $\gamma=10$. Since it is assumed that enhanced node domain size=4 and the start point of the movement is the boundary of one enhanced node domain, the signalling cost increases sharply when MN crosses enhanced node domain ($x=1, 5, 9, 13...$ in the figure). This is because of the location update to HA, CN and location update for fast handovers between ENs. Also, with security mechanism introduced, it generates a noticeable amount of signalling cost, if the MN moves across EN domain. It can be also noticed that the signalling cost is generally higher with large value of $\gamma$ than with small $\gamma$. This is because that larger variance of the AR residence time indicates the probability that an MN remains in AR domain for a shorter time. In other words, MN is with higher mobility rate. And the security mechanism introduces more signalling (about 1/3-2/3 of the location update cost in F-HMIP) on the location update cost.

Figure 6.13 Probability v.s number of ARs crossed between two consecutive packet arrivals. $T_c$ follows Erlang distribution with $\lambda c=3$ and $m=2$. Tm follows Gamma distribution with $\lambda m=30$ and varying $\gamma$ values: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$; (4) $\gamma=10$.

Figure 6.13 shows probability distribution of the number of ARs crossed between two consecutive packet arrivals, indicating the impact of variance in Tm. It is assumed that Tc follows Erlang distribution with $\lambda c=3$ and $m=2$, and Tm follows Gamma distribution with $\lambda m=30$ and varying $\gamma$ values. Figure (1), (2), (3) and (4) shows the results with different $\gamma$ values: (1) $\gamma=0.1$; (2) $\gamma=0.5$; (3) $\gamma=1$ and (4) $\gamma=10$. If AR residence time is with a large variance, a high number of ARs crossed two consecutive packet arrivals occupies a larger amount of the overall number of AR crossed, compared to the AR residence time with small variance. For example, the probability
of MN crossing five ARs between two consecutive packet arrivals is the highest when \( \gamma=10 \) and is the lowest when \( \gamma=0.1 \).

![Figure 6.14](image)

**Figure 6.14** Signalling cost (LU cost and LU+security cost) v.s number of ARs crossed between two consecutive packet arrivals. Tc follows Erlang distribution with \( \lambda c=3 \) and \( m=2 \). Tm follows Gamma distribution with \( \lambda m=30 \) and varying \( \gamma \) values: (1) \( \gamma=0.1 \); (2) \( \gamma=0.5 \); (3) \( \gamma=1 \); (4) \( \gamma=10 \).

Figure 6.14 shows the impact of number of ARs crossed between two consecutive packet arrivals on signalling cost (Location update cost in F-HMIP and total signalling cost with security mechanism enabled). The unit signalling cost is the cost for transmitting a local BU to EN, as defined in section 6.5.2. In [99], Tc is assumed to follow Erlang distribution and Tm follows Gamma distribution, which will also be applied here. Tc follows Erlang distribution with \( \lambda c=3 \) and \( m=2 \), and Tm follows Gamma distribution with \( \lambda m=30 \) and varying \( \gamma \) values: (1) \( \gamma=0.1 \); (2) \( \gamma=0.5 \); (3) \( \gamma=1 \); (4) \( \gamma=10 \). The results illustrate the similar trend as in Figure 6.12. The signalling cost in Figure 6.14 is generally higher than that in Figure 6.12. This is because that for the same number of ARs crossed between consecutive packet arrivals, the probability for Tc with Erlang distribution is higher than for Tc with Exponential distribution (as shown in Figure 6.11 and Figure 6.13). It is also shown in the figure that the signalling cost increases sharply when the MN crosses EN domains and the security mechanism introduces around 50% more overhead than the standard F-HMIPv6 location update cost. It can also be noticed from Figure 6.12 and Figure 6.14 that the probability behaviour is quite similar, regardless the Tc's probability density function (pdf) choice of exponential distribution (Figure 6.12) or Erlang distribution (Figure 6.14).
Figure 6.15 shows the impact of call to mobility ratio $\rho = \lambda_c/\lambda_m$ on signalling cost. $T_c$ follows Erlang distribution $m=2$. $T_m$ follows Gamma distribution with $\gamma=0.1$. It should be noted that the signalling cost here is not weighed by probability as in Figure 6.12 and Figure 6.14. It is shown in the figure that signalling cost decreases as $\rho$ increases. Higher $\rho$ indicates less ARs crossed between two call arrivals, which results in less signalling cost. Therefore, signalling cost decreases as call to mobility ratio increases. It can be also noticed that security mechanism introduces extra signalling cost, and the gain of total signalling cost with security mechanism to location update cost in F-HMIP reduces as $\rho$ increases. This is because that smaller $\rho$ indicates MN crossing more ARs/ENs between two packet arrivals, which would result in more security signalling cost. And the security mechanism adds particularly more signalling cost when the handover is performed between EN domains. If $\rho$ is large enough (close to 100), the MN is crossing limited number of ARs between two packets arrivals, which means the probability that it performs handover between ENs is very low. Therefore, the gain of total signalling cost is getting lower if larger $\rho$ is considered. The same experiment has been carried out to investigate the case if different values of $\gamma$ is chosen ($\gamma=10$), and the similar trend is shown in the result.

![Figure 6.15](image)

Figure 6.15  Signalling cost v.s call to mobility ratio $\rho = \lambda_c/\lambda_m$. $T_c$ follows Erlang distribution with $m=2$ and $T_m$ follows Gamma distribution with $\gamma=0.1$.

### 6.7 Discussions

In section 6.6, the performance of the proposed security mechanism is evaluated. The proposed solution is compared with the F-HMIP protocol in terms of the signalling cost. The signalling cost
evaluated against two parameters: AR crossed between two consecutive packet arrivals and call to mobility ratio. The results indicate that the proposed security mechanism generates about 1/3-2/3 more signalling cost comparing to the F-HMIP registration cost. The F-HMIP protocol is chosen as benchmark here because no similar mechanisms are proposed to secure fast handover in HMIPv6 networks in my knowledge. Please be noted that it is considered in the simulation that security mechanism is enabled for every single handover the MN performs between ARs/ENs. Thus, it is the worst case in terms of signalling overhead. However, it might not be necessary that the keys are established between every previous AR/EN and new AR/EN. Thus, the signalling overhead introduced by security mechanism would be less. There are two reasons for the extra signalling cost:

- Extra signalling messages. For the handover within one EN domains, the FHK Req./Resp. messages are introduced for the EN to generate fast handover keys to be shared between PAR and NAR. For the handover across two EN domains, the AAAF server is involved to generate fast handover keys to be shared by PEN and NEN. AAA Req./Resp. commands are introduced to carry the keying materials/keys. With the security mechanism enabled, it adds more signalling overhead to the fast handover registration messages.

- Modification to the fast handover registration messages. The FBU messages are proposed to contain more mobility options to carry information that EN/AAAF server need for key generation and distribution. However, the modification to the standard registration messages does not introduce as much overhead as the extra security signalling messages, such as AAA Req.

It is considered in the simulation that the key size is 16 bytes. The signalling cost would be slightly different if different key size is chosen. However, the difference would not be noticeable, because the signalling overhead is dominated by the AAA messages. AAA solution is not light-weighted, because of DIAMETER protocol’s format and the amount of AVPs carried in DIAMETER message.

A larger EN size (for instance, 7 ARs in each EN domain) is also investigated in the simulation, and similar trends are shown in the results.

The proposed security mechanism does not have too much negative impact on the handover latency, as the security signalling are integrated with the mobility signalling. The security mechanism does not introduce more round-trip-time delays. More detailed analysis is provided in Appendix D.
Chapter 7

7 Conclusions and Future Work

In the final chapter, I will highlight the work presented in the thesis and demonstrate the impact of the work on future design. A few directions for possible future improvements and research issues are also listed in section 7.2.

7.1 Conclusions

The focal point of work in the thesis is to address security challenges in HMIPv6 networks and to evaluate the impact of security mechanisms on the mobile networks in terms of extra signalling cost introduced. The security threat analysis is carried out based on the proposed architectural framework and the corresponding security requirements are drawn. The proposed solutions basically aim at mitigate the security risks when the mobile node is roaming within or across networks. Handovers can be classified into micro-mobility handover, macro-mobility handover and network-level handover. The proposed solutions target at providing security mechanisms for network-level handover, micro-mobility handover and fast handovers for both micro-mobility and macro-mobility.

For the network-level handover, an enhanced AAA solution for authenticated access control is proposed to provide the mobile node authenticated network access. The mechanism also generates key to be used between serving and target enhanced nodes across access networks. The session key can also be used to secure communication between mobile node and enhanced node in the target access network. The proposed procedure is performed before the mobile node connects to the target access network, thus, it minimises the negative impact on handover disruption time. In the traditional Mobile IP/AAA solution, it usually generally takes an extra round-trip-time to authenticate the mobile node with the AAA sever in its home network. The performance of the proposed mechanism is evaluated using analytical models, namely random walk and fluid flow. The proposed solution is compared with the traditional Mobile IP/AAA solution in terms of signalling cost. It has been concluded that the proposed mechanism introduces slightly more signalling overhead than the traditional Mobile IP/AAA solution. This is reasonable since the proposed security provides functions of distributing keys between neighbouring access networks
and localizing security credentials in the target access network, which do not exist in the traditional Mobile IP/AAA solution. And the proposed solution also has the advantage of minimizing extra handover disruption time.

For micro-mobility handover, it is proposed in the thesis an enhanced key management scheme for securing handovers within one enhanced node domain. In order to secure the micro-mobility registration procedure, handover key needs to be established between enhanced node, access router and mobile node, before the handover is performed. Previously, the key generation takes place every time the mobile node changes its point of attachment to the network, thus, large overhead and extra handover disruption time are introduced due to the frequent distribution of key/keying materials. It is proposed in the thesis an enhanced key management scheme to generate a bunch of handover keys at one time, when the mobile node first enters an enhanced node domain. The efficient key management scheme reduces the negative impact of key generation/distribution on micro-mobility handover disruption time. Since, the handover key generation does not need to be performed as long as the mobile node remains in the same enhanced node domain. The performance of the proposed mechanism is evaluated using fluid flow and random walk models. The proposed mechanism is compared with the previous solution on the parameter of signalling cost. The results demonstrate that the proposed mechanism generates more signalling cost in some scenarios and less signalling cost in others. For instance, if the HKS is located in the visiting network domain, the proposed security mechanism generates slightly more signalling overhead than the previous mechanism, and if the HKS is located in another domain, the proposed security mechanism can result in less signalling overhead, depending on the distance between the two domains. There are a few other factors that dominate the overall signalling cost, such as enhanced node domain size, the handover key size, etc. The impact of these factors is also investigated in the evaluation. The handover keys can be used to secure the registration messages, such as BU, etc, but also to protect the important QoS messages, such as QoS combined BU, etc.

Fast handover is required in both of micro-mobility and macro-mobility handovers in order to reduce the handover delay and packet loss rate. To enhance HMIPv6 based networks with fast handover mechanism, not only fast handover between neighbouring ARs within one enhanced node domain is required, but also fast handover between neighbouring enhanced nodes is necessary. Since the macro-mobility handover between enhanced node domains evokes global registration to the home network which usually cause noticeable delay, the fast handover mechanism is even more necessary. It is specified in the thesis the details of HMIPv6 and FMIPv6 integration (F-HMIPv6), including both of micro and macro mobility handovers. And based on F-HMIPv6 networks, the security mechanism is proposed to secure the fast handover between
ARs/enhanced nodes. The fast handover key is established between previous AR/EN and new AR/EN, thus, the fast handover registration messages between ARs/ENs can be secured. More importantly, the context transfer messages between previous mobility agents and new mobility agents, for the purpose of prompting "smooth handover", can be protected using the fast handover keys. One example of the context transfer is the QoS context transfer message between previous EN and new EN, to allow the mobile node smooth handover experience with minimal service degradation. Performance of the proposed security mechanism is evaluated in terms of the signalling cost. The signalling overhead introduced by security mechanism is quantified using the analytical model and compared with F-HMIPv6 mobility signalling overhead. The worst case is considered in the simulation, which is the scenario security mechanism is enabled for every single handover the MN performs between ARs/ENs.

Reduction of signalling load and handover delay associated with IP mobility management is one of the significant challenges to most of IP mobility support protocols. Much work has been carried out by researchers world widely and also by IETF working groups. As an invisible function, security also introduces extra signalling overhead and handover disruption time. And, AAA solution is always claimed to be heavy and time-consuming. Thus, the conflict of introducing security mechanisms to Mobile IP networks and minimizing the negative impact of security is becoming a focal point for future system design. Especially, when MIPv6 or HMIPv6 is deployed to a large-scale wireless mobile network, such as CDMA 2000, the efforts toward reducing the negative impact are expected to be more emphasized because a huge number of mobile nodes will be served in the network. The work carried out in the thesis gives particular attention on minimizing the negative impact of security mechanisms on the network. And innovatively, the signalling overhead introduced by AAA-based security solutions is quantified. It provides a good guidance for future security design using AAA infrastructure.

7.2 Future Work

A few directions for possible future work which could improve the work presented in the thesis and a couple of interesting research issues are presented in this section.

1. Localized AAA solution

The enhanced AAA solution for handover across access networks is proposed in chapter 4. In this solution, the AAAH server distributes the keys/keying materials to the serving and target AAAF servers in the visited network, and also to the MN. Thus, the MN shares the secret with the AAAF server in the target access network. This process localizes the AAA solution so that the MN does
not need to traverse the wide internet to the AAA server in its home network in the future. However, the concept of shadow registration, as explained in section 4.3.4, requires the local SA to be established a priori the possible handover. A hierarchy of AAA servers is usually implemented in shadow registration. Not only the AAAF server placed in the EN level needs to share SA with MN, but also the local AAA servers (AAAL) collocated with the ARs need to establish SA with the MN. The possible future works remain: How to extend the proposed mechanism to distribute the SAs from AAAF server to the AAAL servers? And is the dynamic distribution of SAs to AAAL servers possible so that the SAs do not need to be distributed to all of the AAAL servers at one time? Resolving the two problems would make the proposed solution fully compliant with the concept of shadow registration.

2. Dynamic key management scheme

The enhanced key management scheme is proposed in chapter 5, which generates a bunch of handover keys to be shared between MN, all of the ARs in one EN domain, and the EN. One interesting scenario draws particular attention is: if the enhanced node domain is reconfigured with a joining AR, how does the proposed mechanism proceed to establish handover key between the new AR and MN? A possible solution would be the combination of the proposed mechanism and the previous mechanism. When the MN is about to handover to another AR and discovers that it does not share a key with the AR, it sends a handover key request message to the EN, as defined in the previous key generation mechanism. The proposed mechanism can be improved by the dynamic scheme.

3. Fast handover interworking with context transfer protocols

The proposed mechanism aims to establish keys between neighbouring ARs/ENs to protect the fast handover registration messages on/and context transfer signalling. The 'seamoby' working group in IETF has been working on defining a new protocol which allows state information to be transferred between edge mobility devices during fast handover procedure. Examples of state information that could be useful to transfer are AAA information, security context, QOS properties assigned to the user, etc. An interesting direction for future work would be specify the details on interworking of fast handover context transfer protocol and the proposed fast handover key management scheme. And it is also important to evaluate efficiency of the interworking.

4. Kerberos mechanism

Kerberos is an authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secured manner. It operates at a client–server model and it provides mutual authentication which means both the user and the server can verify
each other's identity. I proposed a Kerberos-based method to secure handovers in HMIPv6 (see Appendix F). Although Kerberos protocol [100] is a mutual protocol with many improvements and extensions, such as extension proposed in [101], the lack of integration with Mobile IP protocols and its heavy signalling load resulted by mutual authentication remain as the obstacles. Further work can be carried out on exploring details on Kerberos/Mobile IP integration and possible methods of simplifying the procedure to reduce the signalling overhead.

5. DIAMETER implementation

The AAA framework and DIAMETER protocol are used in the proposed solutions. It will be useful if the proposed mechanisms are implemented in test bed such as the work done in [102]. The guidelines for DIAMETER implementation are specified by IETF in [103]. And there are a few existing DIAMETER implementation, such as “openDiameter”, “IntelliNet’s Accelero DIAMETER”, etc. In order to implement the proposed solutions, there are some requirements. Firstly, there should be DIAMETER infrastructure with servers supporting the DIAMETER base protocol. Secondly, extra AVPs, as defined in each solution, should be supported in the DIAMETER client and servers. Thirdly, DIAMETER client should be compatible with Mobile IP protocol, which indicates DIAMETER client should be able to convert Mobile IP message into DIAMETER message. Lastly, security algorithms, such as key generation algorithm and hashing functions, should be supported by DIAMETER servers accordingly.

6. Integration with QoS

The initial integration of security and QoS is achieved in the thesis, by securing important QoS messages explained in Appendix A and E. However, further integration can be investigated, in terms of integration of security and QoS signalling, ensuring the delivery of essential security messages, etc. It would be also interesting to evaluate the overall signalling overhead introduced by security, mobility management and QoS.

7. Contributions to IETF

In Chapter 4 and 6, new AAA solutions are proposed for securing HMIPv6/FMIPv6 networks, which can be contributed to Mobility Extensions for IPv6 (MEXT) or AAA working groups in IETF. In Chapter 5, an enhanced key management scheme for HMIPv6 network is proposed, which provides improvement for the mechanism proposed in an internet draft [86]. In the future, new internet drafts can be submitted based on the work presented in this thesis.
Bibliography


162


<table>
<thead>
<tr>
<th>Bibliography</th>
</tr>
</thead>
<tbody>
<tr>
<td>169</td>
</tr>
</tbody>
</table>


Appendix A

The Combined Mobility and QoS Framework for Inter Access Network Handovers

As part of the Mobile VCE Ubiquitous Services Project, a combined mobility and QoS framework is proposed in [55]. The combined framework can be applied for handover across access networks.

The enhanced nodes located within each access network will communicate with each other through a common inter domain signalling protocol to share mobility and QoS information. For example, during an inter-access handover, the mobile node will be moving from one access point of one network to the access point of another network. Within the current internet architecture, this handover will create large delay during the handover. However, with the presence of the enhanced nodes as well as the exchange and translation of mobility information between them, the handover procedures can be optimised, thus reducing the overall handover delay. The same applies with the re-establishment of the quality of service. A mobile node attached to one network will have its QoS profile stored with that network. As it moves into the new network (with different QoS mechanisms) a fresh profile will need to be created, increasing the overall handover delay. However, with the presence and communication of the enhanced nodes the QoS profiles can be translated from one network to another eliminating the need to create new profiles resulting in faster and more efficient handovers. By using the ENs, I aim to make the two networks appear virtually as a single network allowing them to cooperate seamlessly.

Three different phases are proposed in this new mechanism. The Signalling details are shown in Figure 1.

1. The initial login
2. The handover preparation
3. The handover execution

**Login phase**

During the login phase the MN establishes a binding update with the EN, the EN performs the functionality of Mobility Anchor Point (MAP) as in Hierarchical Mobile IPv6 providing local
mobility. The MN is required to have all its sessions served through the EN hence, the EN is required to hold the QoS states such as the DiffServ code point for each of the MN session packets. The EN knowing the Radio Access Technology used in the network (i.e. WLAN, WiMAX, UMTS etc), is expected to store the DiffServ code points mapping that the AR/AP will use for the established session. During the login phase the EN obtains the mobility update (LCoA) and also the unique Home address of the MN for its identification and when a session is established, the EN holds the QoS states of each session of the MN. Hence, in the login and session establishment phase the EN is expected to obtain these Mobility and QoS context of the MN. This information will be transferred to the new network during an inter-access network handover.

**Handover Preparation Phase**

The handover preparation phase forms the core of the proposed mechanism. It's aimed at reducing the handover delay during an IP handover execution by combining mobility and QoS signalling. Thus, the handover preparation phase occurs just before the handover execution phase. It is assumed that the MN is in the coverage of both the networks, i.e. the two networks are overlapping sufficiently for the MN to perform the handover preparation. The overlapping is necessary for the MN to receive signal from the target network before it loses coverage from the serving network. The required size of the overlap between the coverage of the two networks depends on the max speed of the MN. The faster the MNs move a greater overlapping is required for the handover to complete. Once the MN is under the coverage of the target network the target AR is chosen from the received router advertisement. This router advertisement contains information of the target EN the mobile node is required to connect to. Upon receiving that router advertisement the MN forwards a handover preparation message to the Serving EN. This message also includes a copy of the router advertisement message received from the target AR which contains the target EN IP address as shown in Figure 1.

In turn, if not already available, the serving EN collects the QoS context of the MN (step 3 and 4) and sends a combined Mobility and QoS context transfer binding update (step 5) to the target EN. The mobility context will include the binding information of the MN i.e. the home address. Moreover, to minimise the packet dropping probability during the inter-access network handovers, the EN will establish a temporary tunnel between the serving EN and the target EN as shown in Figure 1. This occurs with the combined mobility and QoS binding update. To minimise wastage of resources, this temporary tunnel can be set up but not executed until the MN performs the handover or is just about to perform a handover. This information can be obtained from the L2 triggers as the MN starts a L2 handover.
After receiving the combined mobility and QoS context transfer from the serving EN, the target EN processes the information and communicates with the Bandwidth Broker in the target network to obtain call admission to the MN’s existing sessions and to calculate the path with the right QoS towards the target AR for the MN. This process is shown in steps 6, 7, 8 and 9 in Figure 1. This ensures that the QoS mapping and state information for the existing sessions from the previous access networks are converted into the new access network’s requirements and are setup before the actual handover. The mobility tunnel between the serving EN and the target EN is established in this phase (step 9). An acknowledgement to the serving EN for this combined mobility and QoS update is sent back which is then forwarded to the MN while is still connected to the serving access network. This gives the signal for the MN to execute the controlled handover to the new access network.

**Handover Execution Phase**

At the execution of the handover from the serving access router to the new target access router, the MN sends the final binding update to the EN with its home address as the unique identifier to associate it with the established QoS and Mobility updates. The temporary tunnel set up between the serving and target EN forwards all packets to the new EN. These packets are then tunnelled to the MN at the target AR. During this time a global binding update is sent by the EN to alert the HA and CN of the change in regional address of the MN. Once this update is processed the HA forwards the packets directly to the target network and the temporary tunnel between the old and new EN expires and is torn down. Using this combined signalling and exploiting the cooperative features between the networks, the inter-network handover can be optimised resulting in a smooth handover for the MN.
Figure 1 Inter Access Networks Signalling
Appendix B

DIAMETER/MIP Application-AMR and AMA Commands

The AAA Working Group in IETF defined the DIAMETER application for Mobile IP, enabling
the mobility agent to interact with AAA entities. AA-Mobile-Node-Request (AMR) and AA-
Mobile-Node-Answer (AMA) commands are two of the important commands for
DIAMETER/MIP integration.

I. AMR command

The AMR command, indicated by the Command-Code field set to 260 and the 'R' bit set in the
Command Flags field, is sent by an attendant (i.e., the mobility agent), acting as a Diameter client,
to an AAAF in order to request the authentication and authorization of a MN. The mobility agent
uses information found in the registration request to construct the following AVPs, to be included
as part of the AMR:

- Home Address (MIP-Mobile-Node-Address AVP)
- Home Agent Address (MIP-Home-Agent-Address AVP)
- Mobile Node NAI (User-Name AVP)
- MN-HA Key Request (MIP-Feature-Vector AVP)
- MN-FA Key Request (MIP-Feature-Vector AVP)
- MN-AAA Authentication Extension (MIP-MN-AAA-Auth AVP)
- Foreign Agent Challenge Extension (MIP-FA-Challenge AVP)
- Home Agent NAI (MIP-Home-Agent-Host AVP)
- Home AAA server NAI (Destination-Host AVP [DIAMBASE])
- Home Agent to Foreign Agent SPI (MIP-HA-to-FA-SPI AVP)

If the MN's home address is zero, the FA or HA must not include a MIP-Mobile-Node-Address
AVP in the AMR. If the HA address is zero or all ones, the MIP-Home-Agent-Address AVP
must not be present in the AMR.

If a HA is used in a visited network, the AAAF may set the Foreign-Home-Agent-Available
flag in the MIP-Feature-Vector AVP in the AMR message to indicate that it is willing to assign a
HA in the visited realm.
If the MN's home address is all ones, the FA or HA must include a MIP-Mobile-Node-Address AVP, set to all ones.

If the MN includes the HA NAI and the home AAA server NAI, the FA must include the MIP-Home-Agent-Host AVP and the Destination-Host AVP in the AMR.

The Format of AMR command is defined in DIAMETER/MIP application. And the complete message fields are listed as follows. It should be noted that not all of the AVPs must be present in the DIAMETER message. Some of the AVPs may not be present, and there may be more than one of certain AVP in one message. The {} AVP is mandatory, and [] AVP is optional.

<AMR> ::= < Diameter Header: 260, REQ, PX > < Session-ID > { Auth-Application-Id } { User-Name } { Destination-Realm } { Origin-Host } { Origin-Realm } { MIP-Reg-Request } { MIP-MN-AAA-Auth } [ Acct-Multi-Session-Id ] [ Destination-Host ] [ Origin-State-Id ] [ MIP-Mobile-Node-Address ] [ MIP-Home-Agent-Address ] [ MIP-Feature-Vector ] [ MIP-Originating-Bear-AAA ] [ Authorization-Lifetime ] [ Auth-Session-State ] [ MIP-FA-Challenge ] [ MIP-Candidate-Home-Agent-Host ] [ MIP-Home-Agent-Host ] [ MIP-HA-to-FA-SP ] *[Proxy-Info] *[Route-Record]*[AVP]

II. AMA command

The AMR command, indicated by the Command-Code field set to 260 and the 'R' bit cleared in the Command Flags field, is sent by the AAAH in response to the AMR message. The User-Name may be included in the AMR if it is present in the AMR. The Result-Code AVP must be included in the command, containing one of the values defined by DIAMETER/MIP application.

An AMR message with the Result-Code AVP set to "DIAMETER_SUCCESS" must include the MIP-Home-Agent-Address AVP, and must include the MIP-Mobile-Node-Address AVP, and includes the MIP-Reg-Reply AVP if and only if the Co-Located-Mobile-Node bit was not set in the MIP-Feature-Vector AVP. The MIP-Home-Agent-Address AVP contains the HA assigned to the MN, while the MIP-Mobile-Node-Address AVP contains the home address that was assigned. The AMR message must contain the MIP-FA-to-HA-MSA and MIP-FA-to-MN-MSA if they were requested in the AMR. The MIP-MN-to-HA-MSA and MIP-HA-to-MN-MSA AVPs must be present if the session keys were requested in the AMR and the Co-Located-Mobile-Node bit was set in the MIP-Feature-Vector AVP.

The complete AMR command fields are listed as follows,

<AMR> ::= < Diameter Header: 260, PX > < Session-Id > { Auth-Application-Id } { Result-Code } { Origin-Host } { Origin-Realm } [ Acct-Multi-Session-Id ] [ User-Name ] [
Authorization-Lifetime ] [ Auth-Session-State ] [ Error-Message ] [ Error-Reporting-Host ] [ Re-
Auth-Request-Type ] [ MIP-Feature-Vector ] [ MIP-Reg-Reply ] [ MIP-MN-to-FA-MSA ] [ MIP-
MN-to-HA-MSA ] [ MIP-FA-to-MN-MSA ] [ MIP-FA-to-HA-MSA ] [ MIP-HA-to-MN-MSA ] [ MIP-
MSA-Lifetime ] [ MIP-Home-Agent-Address ] [ MIP-Mobile-Node-Address ] *[ MIP-
Filter-Rule] [Origin-State-Id] *[Proxy-Info] *[AVP]
# Appendix C

## Table of Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>Unit transmission costs in a wired link</td>
<td>1</td>
</tr>
<tr>
<td>$K$</td>
<td>Unit transmission costs in a wireless link</td>
<td>2</td>
</tr>
<tr>
<td>$\rho$</td>
<td>MN's density</td>
<td>$0.0002$ users/m$^2$</td>
</tr>
<tr>
<td>$R$</td>
<td>Number of rings of enhanced node domains in one access network</td>
<td>3</td>
</tr>
<tr>
<td>$q$</td>
<td>Residence probability</td>
<td>0.2</td>
</tr>
<tr>
<td>$l_w$</td>
<td>Perimeter of the enhanced node domain</td>
<td>500</td>
</tr>
<tr>
<td>$N_{CN}$</td>
<td>Number of CN</td>
<td>2</td>
</tr>
<tr>
<td>$PC_x$</td>
<td>Processing cost at network entity X</td>
<td>$PC_x=04$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$PC_x=6$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$PC_x=12$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$PC_x=24$;</td>
</tr>
<tr>
<td>$D_{xy}$</td>
<td>Distance between network entity $x$ and $y$</td>
<td>$D_{xy}=2$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$D_{xy}=6$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$D_{xy}=4$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$D_{xy}=1$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$D_{xy}=6$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$D_{xy}=-20$;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$D_{xy}=1$;</td>
</tr>
</tbody>
</table>
### Appendix C

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_s$</td>
<td>Session key generation cost</td>
<td>6</td>
</tr>
<tr>
<td>$H_{mod}$</td>
<td>Hashing cost</td>
<td>3</td>
</tr>
<tr>
<td>$E_{des}$</td>
<td>Encryption/Decryption cost using DES</td>
<td>9</td>
</tr>
<tr>
<td>$C_{x-y}$</td>
<td>the coefficient of transmission cost for BU/BA (to HA) from entity $x$ to $y$</td>
<td>$c_{HA-x} = 0.78$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_{BA-x} = 0.78$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_{x-x} = 0.78$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_{x-HA} = 1.33$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_{x-BA} = 1.33$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_{x-x} = 1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_{x-x} = 1$</td>
</tr>
</tbody>
</table>

**$S_{ij}$ Coefficients:**

- Transmission cost of security signalling in a wireless and wired link between corresponding entities is $S_{ij}$ times of $c_{ij}$ (previous security mechanism).
- $S_{ij} = 3.72;
- S_{12} = 5.33;
- S_{21} = 1.44;
- S_{11} = 1$;
- $S_{22} = 1.44;
- S_{22} = 1$;
- $S_{31} = 5.33;
- S_{32} = 3.72;
- S_{41} = 5.33;
- S_{42} = 3.72;

**$S_{ij}$ Coefficients:**

- Transmission cost of security signalling in a wireless and wired link between corresponding entities is $S_{ij}$ times of $c_{ij}$ (the proposed security mechanism).
- $S_{ij} = 2.11;
- S_{11} = 1.36;
- S_{21} = 2.11;
- S_{22} = 1.36;
- S_{31} = 6.07;
- S_{32} = 5;
- S_{41} = 6.07;
- S_{42} = 5;
$S' = 3.17$;
$S'' = 3.17$;

### Table I - The Values of Parameters: Chapter 4

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N(K)$</td>
<td>Domain size</td>
<td>20</td>
</tr>
<tr>
<td>$S$</td>
<td>AR area</td>
<td>$10 \text{ km}^2$</td>
</tr>
<tr>
<td>$T$</td>
<td>Binding lifetime. $T_{EN}$, $T_{HA}$ and $T_{CN}$ are the binding lifetimes for the enhanced node, the HA and the CNs, respectively. It is assumed that $T_{EN} = T_{HA} = T_{CN} = T$.</td>
<td>0.3 hr</td>
</tr>
<tr>
<td>$v$</td>
<td>Average speed of an MN</td>
<td>5 or 20 km/hr</td>
</tr>
<tr>
<td>$r$</td>
<td>Ratio of the network scale</td>
<td>0.2</td>
</tr>
<tr>
<td>$c$</td>
<td>Average number of CNs when a MN moves into/out of a given enhanced node domain</td>
<td>0.1</td>
</tr>
<tr>
<td>$\delta$</td>
<td>Ratio of an MN’s average binding time for the CNs to its average domain residency time</td>
<td>0.1</td>
</tr>
<tr>
<td>$b$</td>
<td>Link hops between the first and the second layer nodes in the same network domain</td>
<td>3</td>
</tr>
<tr>
<td>$k$</td>
<td>Coefficient of transmission cost over wireless link. The unit transmission cost over a wireless link is $k$ times of that over a wired link</td>
<td>2</td>
</tr>
<tr>
<td>$HK$ size</td>
<td>Handover Key Size</td>
<td>128 bits–16 bytes</td>
</tr>
<tr>
<td>$w_d$</td>
<td>Wireless links</td>
<td>1</td>
</tr>
</tbody>
</table>

$BW^X_{BU}$: Signalling bandwidth consumption generated by message $X$ (BU/BA/BR) from/to entity $Y$ (EN/HA/CN)

- $BW^BR_{BU}$: BU message to EN: 72 bytes
- $BW^BA_{BU}$: BA message from EN: 56 bytes
- $BW^BR_{BA}$: BU message to HA: 72 bytes
- $BW^BA_{BA}$: BA message from HA: 56 bytes
- $BW^BR_{HA}$: BU message to CN: 96 bytes
- $BW^BA_{HA}$: BA message from CN: 72 bytes
- $BW^BR_{EN}$: BR message from EN: 48 bytes
- $BW^BA_{HA}$: BR message from HA: 48 bytes
Appendix C

\(BW_{BR}^{\text{it}}\): BR message from CN 48 bytes

\(BW_{x}^{\text{it}}\)

- Signalling bandwidth consumption generated by message X (HKReq./HKResp./AAAReq./AAAResp.) in previous security mechanism
  - \(BW_{\text{HKReq.}}^{\text{it}}\): HKReq. message MN\(\rightarrow\)AR\(\rightarrow\)EN 184 bytes
  - \(BW_{\text{HKResp.}}^{\text{it}}\): HKResp. message AR\(\rightarrow\)MN 104 bytes
  - \(BW_{\text{HKResp.}}^{\text{it}}\): HKResp. message EN\(\rightarrow\)AR 96 bytes
  - \(BW_{\text{AAAReq.}}^{\text{it}}\): AAAReq. message EN\(\rightarrow\)HKS 604 bytes
  - \(BW_{\text{AAAResp.}}^{\text{it}}\): AAAResp. message HKS\(\rightarrow\)EN 248 bytes

\(BW_{y}^{\text{it}}\)

- Signalling bandwidth consumption generated by message X (HKReq./HKResp./AAAReq./AAAResp.) in the proposed security mechanism
  - \(BW_{\text{HKReq.}}^{\text{it}}\): HKReq. message MN\(\rightarrow\)AR\(\rightarrow\)EN 192 bytes
  - \(BW_{\text{HKResp.}}^{\text{it}}\): HKResp. message AR\(\rightarrow\)MN 88+20*N(K) bytes
  - \(BW_{\text{HKResp.}}^{\text{it}}\): HKResp. message EN\(\rightarrow\)serving AR 80+20*N(K) bytes
  - \(BW_{\text{HKResp.}}^{\text{it}}\): HKResp. message EN\(\rightarrow\)other ARs, except for the serving AR 72 bytes
  - \(BW_{\text{AAAReq.}}^{\text{it}}\): AAAReq. message EN\(\rightarrow\)HKS 604+28*N(K) bytes
  - \(BW_{\text{AAAResp.}}^{\text{it}}\): AAAResp. message HKS\(\rightarrow\)EN 216+48*N(K) bytes

---

Table II the Values of Parameters: Chapter 5

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\delta)</td>
<td>The unit transmission cost in a wired link. The unit transmission cost is the transmission cost for local BU message to enhanced node</td>
<td>1</td>
</tr>
<tr>
<td>(M)</td>
<td>The transmission cost over a wireless link is (m) times the cost over a wired link</td>
<td>2</td>
</tr>
<tr>
<td>(S)</td>
<td>Distance (number of hops) between enhanced node and HKS</td>
<td>2</td>
</tr>
<tr>
<td>(K)</td>
<td>Distance (number of hops) between enhanced node and HA</td>
<td>5 or 15</td>
</tr>
<tr>
<td>(L)</td>
<td>Average distance (number of hops) between enhanced node and CN</td>
<td>5</td>
</tr>
<tr>
<td>(C)</td>
<td>Average number of CNs that the MN is communicating with</td>
<td>1</td>
</tr>
<tr>
<td>(\delta_s)</td>
<td>Transmission cost coefficient for mobility signalling from one entity to another</td>
<td></td>
</tr>
</tbody>
</table>
\( \delta_1: \) local BA sent from enhanced node 0.78
\( \delta_2: \) BU sent to HA 1
\( \delta_3: \) BA sent from HA 0.78
\( \delta_4: \) BU sent to CN 1.33
\( \delta_5: \) BA sent from CN 1

\( \delta_{ct} \) Transmission cost coefficient for security signalling from one entity to another, in previous security mechanism

\( \delta_{211} \): HK Req. message MN \( \rightarrow \) AR 2.56
\( \delta_{212} \): HK Resp. message AR \( \rightarrow \) MN 1.44
\( \delta_{221} \): HK Req. message AR \( \rightarrow \) enhanced node 2.56
\( \delta_{222} \): HK Resp. message enhanced node \( \rightarrow \) AR 1.33
\( \delta_{331} \): AAA Req. message enhanced node \( \rightarrow \) HKS 8.39
\( \delta_{332} \): AAA Resp. message HKS \( \rightarrow \) enhanced node 3.44

\( \delta_{ct} \) Transmission cost coefficient for security signalling from one entity to another, in proposed security mechanism

\( \delta'_{211} \): HK Req. message MN \( \rightarrow \) AR 2.67
\( \delta'_{212} \): HK Resp. message AR \( \rightarrow \) MN \( \frac{(88+20*N(K))}{72} \)
\( \delta'_{221} \): HK Req. message AR \( \rightarrow \) enhanced node 2.67
\( \delta'_{222} \): HK Resp. message enhanced node \( \rightarrow \) serving AR \( \frac{(80+20*N(K))}{72} \)
\( \delta'_{331} \): HK Resp. message enhanced node \( \rightarrow \) other ARs, except for the serving AR 1
\( \delta'_{332} \): AAA Req. message enhanced node \( \rightarrow \) HKS \( \frac{(604+28*N(K))}{72} \)
\( \delta'_{332} \): AAA Resp. message HKS \( \rightarrow \) enhanced node \( \frac{(216+48*N(K))}{72} \)

Table III the Values of Parameters : Chapter 5

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n )</td>
<td>Number of CNs communicating with the MN</td>
<td>4</td>
</tr>
<tr>
<td>( N )</td>
<td>EN domains size; number of ARs in one EN domain</td>
<td>4</td>
</tr>
<tr>
<td>( \delta )</td>
<td>Unit transmission costs in a wired link</td>
<td>1</td>
</tr>
<tr>
<td>( \omega )</td>
<td>Coefficient of transmission cost over wireless link. The unit transmission cost over a wireless link is ( \omega ) times of that over a wired link</td>
<td>2</td>
</tr>
</tbody>
</table>
Appendix C

\( P_a \) Processing cost for the location update message at entity \( a \)

\[ P_{AR} = 1 \]
\[ P_{EN} = 2 \]
\[ P_{CN} = 1 \]
\[ P_{MA} = 4 \]

\( S_a \) Processing cost for the security message at entity \( a \)

\[ S_{AR} = 2 \]
\[ S_{EN} = 4 \]
\[ S_{MA} = 4 \]

\( D_{X-Y} \) Distance (number of hops) between network entity \( X \) and \( Y \)

\[ D_{MN-AR} = 2 \]
\[ D_{AR-AR} = 5 \]
\[ D_{AR-EN} = 10 \]
\[ D_{EN-EN} = 20 \]
\[ D_{EN-CN} = 20 \]
\[ D_{EN-RA} = 25 \]
\[ D_{EN-MA} = 10 \]

\( \delta_x \) Transmission cost coefficient for mobility signalling message \( X \) in HMIPv6 to/from entity \( a \)

\[ \delta_{FBU}^{MN} = 0.778 \]
\[ \delta_{FBU}^{PAR} = 1 \]
\[ \delta_{FBU}^{EN} = 0.778 \]
\[ \delta_{FBU}^{CN} = 1.333 \]
\[ \delta_{FBU}^{MA} = 1 \]
\[ \delta_{FBU}^{RA} = 2 \) (MN->PAR)
\[ \delta_{FBU}^{PEN} = 2.333 \) (PAR->PEN)
\[ \delta_{FBU}^{EN} = 1.667 \) (PEN->PAR)
\[ \delta_{FBU}^{EN} = 1.667 \) (PAR->MN)
\[ \delta_{FBU}^{MA} = 1.889 \]
\[ \delta_{FBU}^{CN} = 1.333 \]

\( \delta_x^{AR/EN} \) Transmission cost coefficient for mobility message \( X \) in fast handover between ARs/ENs

\[ \delta_{FBU}^{AR/EN} = 1.333 \]
\[ \delta_{FBA}^{AR/EN} = 1.333 \]
\[ \delta_{Hi}^{AR/EN} = 1.556 \]
\[ \delta_{Hi}^{AR/EN} = 1 \]

\( \varepsilon_{x} \) Transmission cost coefficient for message \( X \) for handovers within one EN domain, with security mechanism enabled. Message \( X \): FBU, FBA, Hi, HaKc.

\[ \varepsilon_{FBU} = 2.778 \]
\[ \varepsilon_{FBA} = 1.333 \]
\[ \varepsilon_{Hi} = 1.556 \]
\[ \varepsilon_{HaKc} = 1 \]
Appendix C

\[ \varepsilon'_{\text{EX}} \text{ Transmission cost coefficient for message X for handovers across EN domains, with security mechanism enabled. Message X: FBU (MN-\text{PAR}), FBU (PAR-\text{PEN}), FBA (PAR-\text{MN}), FBA (PEN-\text{PAR}), HI, H\text{ACK}.} \]

\[ \varepsilon'_{\text{FBU}} = 3 \text{ (MN-\text{PAR})} \]

\[ \varepsilon'_{\text{FBu}} = 3.333 \text{ (PAR-\text{PEN})} \]

\[ \varepsilon'_{\text{FBA}} = 1.667 \text{ (PAR-\text{MN})} \]

\[ \varepsilon'_{\text{FBa}} = 1.667 \text{ (PEN-\text{PAR})} \]

\[ \varepsilon'_{\text{HI}} = 1.089 \]

\[ \varepsilon'_{\text{ACK}} = 1.333 \]

\[ \varepsilon_{1,2,3} \text{ Transmission cost coefficient for FHK Req. (PAR-\text{EN}), FHK Resp. (EN-\text{PAR}), FHK Resp. (EN-\text{NAR}) messages in handovers within one EN domain} \]

\[ \varepsilon_1 = 2.333 \]

\[ \varepsilon_2 = 1.111 \]

\[ \varepsilon_3 = 1.111 \]

\[ \varepsilon'_{1,2,3} \text{ Transmission cost coefficient for AAA Req. (PEN-\text{AAAF}), AAA Resp. (AAAF-\text{PEN}), AAA message (AAAF-\text{NEN}) in handovers across EN domains} \]

\[ \varepsilon'_1 = 5.694 \]

\[ \varepsilon'_2 = 4.056 \]

\[ \varepsilon'_3 = 5.278 \]

---

Table IV The value of parameters: Chapter 6
Appendix D

Handover Delay Analysis

Handover delay broadly consists of two components [48]: link layer establishment delay and signalling delay. In recent implementation of Mobile IPv6 it was found that delay could be as large as 3.6 seconds [104], and the delays involved in Mobile IPv6 are illustrated in Figure 1. After the Layer-2 handover is completed, the Layer-3 delays involved can be classified to [55]: movement detection delay; CoA configuration delay involving Duplicate Address Detection (DAD); binding registration delay to relevant mobility agent (i.e., MAP, HA, CN, etc.), and the extra signalling delay introduced by security, QoS, etc. To minimise the overall handover delay, each of these delay components can be reduced. I aim to minimise the extra signalling delay introduced by security mechanisms, by making use of the intelligence of the EN.

![Diagram showing delay components](image)

**Figure 1: Delay components**

In order to derive the numerical result, the following assumptions are made:

1) The processing time in each entity is negligible since it takes less than 1 ms [105].
2) All control messages for initial registration and handoff are reliably delivered [53].
3) The average RTT between the MN and the AR is \( T_{ar} \) (as shown in Figure 2) which is the average RTT to send and receive a message over the wireless link [53].
4) The average RTT between the AR and the EN is \( T_{ar-en} \) (as shown in Figure 2), which is the average RTT to send and receive a message over the EN domain.
5) The average RTT between the MN and its home network (HA) is $T_h$ (as shown in Figure 2), which is the average RTT to send and receive a message from the home network [106].

6) The average RTT between the MN and the CN is $T_{mc}$ (as shown in Figure 2). This delay varies as the location of CN is different [53].

7) The average RTT between the EN and the AAAF server is $T_{en-aaaf}$ (as shown in Figure 2). This delay depends on the location of the AAAF server.

8) The average RTT between the AAAF server and the AAAF server is $T_{aaaf-aaah}$ (as shown in Figure 2). This delay depends on the location of AAA servers.

9) The average RTT between ARs is $T_{nar-par}$ (as shown in Figure 2), which is the delay between PAR and NAR [106].

10) The average RTT between ENs is $T_{nen-pen}$ (as shown in Figure 2), which is the delay between PEN and NEN.

![Diagram](https://via.placeholder.com/150)

**Figure 2: A simple model for analysis**

The total handover delay is analyzed based on the assumptions and the model illustrated in Figure 2. The three mechanisms presented in Chapter 4, 5 and 6 are analyzed respectively in the following sections.

**Handover between access networks (Chapter 4)**

- Previous mechanism

186
In the previous mechanism, the AAA solution needs to be completed before MN starts the registration procedure, so that the MN can be authenticated by the AAAH server and the relevant keys can be distributed to secure the following registration procedure. The delay to complete AAA process is $T_s + T_{ar-en} + T_{en-aaaaf} + T_{aaaaf-aaah}$. And the delay caused by the registration procedure is $T_s + T_{ar-en} + T_h + T_{mc}$. Thus, the total delay is,

$$\text{Total Delay} = T_s + T_{ar-en} + T_{en-aaaaf} + T_{aaaaf-aaah} + T_s + T_{ar-en} + T_h + T_{mc}$$

- Proposed mechanism

In the proposed mechanism, the AAA solution is completed before the MN connects to the new access router. Therefore, there is no additional delay caused by AAA solutions. The total delay is the delay for the MN to register with the new access network (EN, HA and CN). The delay caused by the registration procedure is $T_s + T_{ar-en} + T_h + T_{mc}$. Thus, the total delay is,

$$\text{Total Delay} = T_s + T_{ar-en} + T_h + T_{mc}$$

The proposed mechanism introduces less delay than the previous mechanism.

**Handover within one access network (Chapter 5)**

- Previous mechanism

In the previous mechanism, MN needs to perform key request to the AAAF server every single time it changes its point of attachment (AR). The key generation/distribution is performed before the registration procedure, thus, the handover key can be used to secure the registration signalling. Therefore, the total delay is consists of two parts: key generation process and registration procedure. The delay caused by key generation is $T_s + T_{ar-en} + T_{en-aaaaf}$. The delay introduced by registration procedure depends on the handover type. If the MN performs handover within one EN domain, the MN only registers with the local EN, thus the delay is $T_s + T_{ar-en}$. If the MN performs handover across ENs, the MN registers not only with EN, but also with HA and CN. Thus, the delay is $T_s + T_{ar-en} + T_h + T_{mc}$. The total delay is,

$$\text{Total Delay} = T_s + T_{ar-en} + T_{en-aaaaf} + T_s + T_{ar-en} + T_h + T_{mc}$$  

**handover within one EN domain**

Total Delay=$T_s + T_{ar-en} + T_{en-aaaaf} + T_s + T_{ar-en} + T_h + T_{mc}$ (handover across EN domains)

- Proposed mechanism

In the proposed mechanism, the key generation is only performed once when the MN first enters a new EN domain. If the MN performs handover within one EN domain, there is no key generation procedure involved, thus, the total delay is only caused by registration to local EN:

$$\text{Total Delay} = T_s + T_{ar-en}$$  

**handover within one EN domain**

If the MN performs handover between EN domains, the total delay is resulted by key generation/distribution and registration procedure (to EN, HA and CN), thus, the total delay is:

$$\text{Total Delay} = T_s + T_{ar-en} + T_{en-aaaaf} + T_s + T_{ar-en} + T_h + T_{mc}$$  

**handover across EN domains**

187
It can be concluded that the proposed mechanism introduces less handover delay than the previous mechanism, in the scenario of handover within one EN domain. For handover across EN domains, the proposed mechanism performs equivalently to the previous mechanism in terms of delay.

**Fast handover within one access network (Chapter 6)**

- **Fast handover without security mechanism (Figure 6.3)**

For handover within one EN domain, the fast handover is performed between PAR and NAR. Thus, the handover delay introduced by fast handover registration is $T_s + T_{nar-par} + T_s/2$. The registration delay introduced by HMIPv6 is $T_s + T_{ar-en}$. Therefore, the fast handover delay is,

$$\max \{ T_s + T_{nar-par} + \frac{T_s}{2}, T_s + T_{ar-en} \}$$

Usually, the registration to local EN takes longer than the fast handover registration between PAR and NAR.

For handover between EN domains, the fast handover is performed between PEN and NEN. The handover delay introduced by fast handover registration is $T_s + T_{ar-en} + T_{nen-pen} + (T_s + T_{ar-en})/2$. The registration delay introduced by HMIPv6 is $T_s + T_{ar-en} + T_h + T_{mc}$. Therefore, the fast handover delay is,

$$\max \{ T_s + T_{ar-en} + T_{nen-pen} + \frac{(T_s + T_{ar-en})}{2}, T_s + T_{ar-en} + T_h + T_{mc} \}$$

Usually, the global registration in HMIPv6 (to HA and CN) takes much longer than the fast handover registration between PEN and NEN.

- **Fast handover with proposed security mechanism (Figure 6.8)**

For handover within one EN domain with proposed security mechanism enabled, the delay is $T_s + T_{nar-par} + T_{ar-en}$. Therefore, the total delay is,

$$\max \{ T_s + T_{nar-par} + \frac{T_s}{2}, T_s + T_{ar-en} \}$$

For handover between EN domains with proposed security mechanism enabled, the delay is $T_s + T_{ar-en} + T_{nen-pen} + \frac{(T_s + T_{ar-en})}{2} + T_{en-aaa}$. Therefore, the total delay is,

$$\max \{ T_s + T_{ar-en} + T_{nen-pen} + \frac{(T_s + T_{ar-en})}{2} + T_{en-aaa}, T_s + T_{ar-en} + T_h + T_{mc} \}$$

It can be concluded that the security mechanism could possibly increase a little bit more handover delay. However, it is possible that the handover delay is equivalent either with or without security mechanism enabled, because the HMIPv6 registration could take even longer. For instance, in the scenario of handover between EN domains, if AAAF server is located very closely to EN, the...
Appendix D

time consumed for key distribution is neglectable comparing to the time to complete global registration.
Appendix E

The Combined Mobility and QoS Mechanism for Handovers between Enhanced Nodes

As part of the Mobile VCE Ubiquitous Services Project, a combined mobility and QoS mechanism is proposed in [11] for handovers between enhanced nodes.

During a handover between mobility agents the location update needs to be sent to the correspondent node (CN) and the home agent. During this, the regional care of address obtained from the mobility agent changes and the packets that the CN transmits to the MN need to be readdressed to the new regional care of address of the new mobility agent. In the proposed architecture the handover will occur between enhanced nodes. Figure 1 shows the signalling for an EN handover scenario with combined Mobility and QoS update. During this handover the destination address stored in the CN changes and as a result, the path from the CN to the EN changes. During the handover period the packets arriving at EN1 are stored and redirected to EN2 where the MN is currently connected. In this way the packet loss is minimised along with the delay associated with macro-mobility.

![Figure 1: Inter ENs handover signalling](image-url)
The combined mobility and QoS mechanism consists of three phases: the initial login (or path setup) phase, the handover preparation phase and the handover execution phase. The handover execution phase is explained in the following paragraph.

**Handover execution phase**

In the case of a handover, if the target AR does not belong to the EN to which the MN is attached, then there is EN change. The handover process is more complex as it involves also the gateway. As shown in Figure 2, when the new EN receives the handover request and detects that the MN is currently attached to different EN, the new EN forwards the message to the old EN which carries out the handover process: it configures the source routing and requests the reservation to the bandwidth broker (BB). After this first phase, a change of EN is triggered by the MN. An EN change message is received by the new EN, which retrieves the MN QoS context from the old EN and sets up a path to the current AR. Once this path has been set up, the new EN sends a EN change message to the gateway, which sets up a path to the new EN. Once the gateway has set up the new path, it requests the BB for resource reservation and DiffServ edge configuration. The DiffServ edge configuration occurs in the case the current DiffServ code-point has been changed, depending on policy management at the BB and the available resources on the segments: gateway - EN and EN – AR.

![Figure 2: Signalling for handover execution with EN change](image-url)
Appendix F

Kerberos-based Method to Secure Handovers in HMIPv6

In a kerberos-based system, two servers are involved:
- AS: authentication server
- KDS: key distribution server

![Figure 1 Kerberos-based authentication method](image)

As illustrated in Figure 1, signalling for kerberos-based method are explained as follows,

1. **Auth Req.**: MN sends an Authentication Request message to serving enhanced node (enhanced node 1). The message includes NAI (user@realm) and a secret master key
   \[ K_{MN-AS} = HMAC_{SHA1}(MN-ID, \ldots) \]

2. **AAA Req.**: enhanced node 1, as an AAA client, issues an AAA request message, which encapsulates the authentication request message, and sends it to AAAF server (also KDS).

3. **AAA Req.**: AAAF server, as a proxy AAA server, forwards the AAA request message to the MN’s AAAH server, according to realm field in NAI.
Appendix F

(4) AAA Resp.: the AAAH server (also the AS), generates a session key $K_s$, which is to be used between KDS and MN. The AAAH server also generates a ticket $T_{MN-KDS} = K_{KDS}[MN'ID, K_s]$, where $K_{KDS}$ is a key that only KDS holds. The AAAH server sends the AAA response message to the AAAF server, including $K_{KDS}[K_{MN-AS}] and K_{MN-AS}[K_s, T_{MN-KDS}]$.

(5) AAA Resp.: The AAAF server shares a secret ($K_{KS}$) with all of the enhanced nodes in the network. It is assumed that the number of enhanced nodes is $N$, therefore, the AAAF server generates $N$ tickets.

$$T_i = K_{KS}[K_{CS}, Intelligent Node i' ID, MN' ID, ...]$$

where, $K_{KS}$ is the key shared by enhanced node $i$ and AAAF server; $K_{CS}$ is the session key generated by the AAAF server and to be shared by enhanced node $i$ and MN.

The AAAF server decrypts $K_s$ using $K_{MN-AS}$, and sends AAA response message to the serving enhanced node. The AAA resp. message includes the following information:

$$K_{MN-AS}[K_s, T_{MN-KDS}], K_s[enhanced node i' ID, K_{CS}, T_i] (i=1, 2, ..., N).$$

(6) Auth Rep.: enhanced node $i$ sends an authentication reply message to MN, including the information in the AAA resp. message. Upon receiving Auth Rep. message, the MN decrypts $K_s$ using $K_{MN-AS}$ and also decrypts $K_s[enhanced node i' ID, K_{CS}, T_i]$ using $K_s$. The MN also stores $T_{MN-KDS}$ and $T_i (i = 1, 2, ..., N)$.

(7) If the MN needs access to enhanced node $i$, it sends Auth req. message to enhanced node $i$, including $T_i (i = 1, 2, ..., N)$ and current time encrypted with $K_{CS}$.

(8) Upon receiving Auth req., the enhanced node $i$ retrieves $K_{CS}$ by decrypting $T_i$ using $K_{KS}$. The enhanced node $i$ uses $K_{CS}$ to decrypt time and increase the value of time by one, and then re-encrypt it with $K_{CS}$ and sends back to MN in an Auth Rep. message.