Security Mechanisms for Delivering Ubiquitous Services in Next Generation Mobile Networks

Yingli Sheng, Haitham Cruickshank
Centre for Communication Systems Research (CCSR)
The University of Surrey, Guildford, Surrey, the United Kingdom
Yingli.Sheng@surrey.ac.uk, H.Cruickshank@surrey.ac.uk

***Abstract*—Delivering ubiquitous services to various users and devices through heterogeneous networks is a major aim in next generation networks. The delivery should be efficient and secure. The support and integration of security, Quality of Service (QoS) and mobility management (MM) in access networks become parts of the essential issues. An Enhanced Node (EN) with a network sub-layer is proposed here to achieve this integration. The architectural framework with ENs located in the IP-based access networks is presented. The focus of this paper is to investigate the challenges of integrating security with QoS and MM, notably the threats and requirements, based on this framework. The solutions are also proposed to provide the authenticated and authorized access control and to secure the handover process.**

Keywords-security; AAA; enhanced node; HMIPv6

I. INTRODUCTION

With the development of Bluetooth, Wifi, WiMAX, Ultra Wide Band (UWB) technologies, ubiquitous access comes closer to reality. However, for the operator, delivery of ubiquitous services today poses many practical challenges [1]. From the network perspective, the key barrier to accessing ubiquitous services arises from the need for security and managing delivery of multiple services within different Quality of Service (QoS) environments through multiple heterogeneous networks [1]. It is therefore essential that different delivery networks should be empowered to operate in a cooperative manner. The presence of intelligence and inter-connection among intelligent entities in such network pose great challenges. Particularly, in order to provide ubiquitous services to the users securely, intelligent entities are required to deliver the security information within the access network and across different access networks.

II. THE BASIC ARCHITECTURAL FRAMEWORK

To address the challenges posed by ubiquitous services, the concept of network support sub-layer, which consists of elements of security, QoS and mobility management (MM) with radio resource management (RRM) hooks, is proposed. The nodes with the support sub-layer are referred to as enhanced nodes (ENs).

A. Enhanced Nodes

1) Functionalities of the Enhanced Nodes

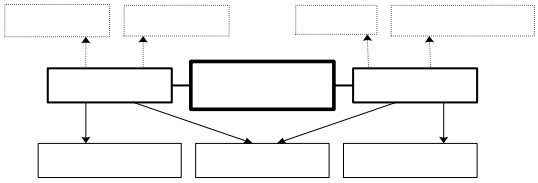


Figure 1. Security related enhanced nodes

The network support sub-layer is located in a small number of ENs in a network. The EN can be an access router (AR), gateway, anchor point, etc. Such selected ENs can be used in the heterogeneous networks comprising security/QoS/MM aware and unaware access networks [1]. With the help of ENs, integration of security, QoS and MM can be achieved. 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, QoS and MM in the various participating networks is a key factor in end-to-end performance [1].

2) Security Related Functions in Enhanced Nodes

The security related ENs are basically normal mobility agents enhanced by specific security functionalities. Fig.1 shows the components and the services provided by the security related EN. The dotted arrow shows the corresponding services provided by the entity. Normally, the security related EN acts as both of the security entity and the mobility agent. As a security entity, it connects to the AAA servers and the ARs. The authenticated access control and the secured handover services can be provided by the security entity. As a mobility agent, it connects to the mobile nodes (MN) and the ARs. It deals with the handover signalling and the basic Mobile IP signalling.

B. The Architectural Framework

Fig.2 shows the architectural framework which our work is based on. Two IP-based access networks with the similar infrastructure are presented. More than one EN with the network sub-layer is located within one access network and they communicate with each other via signalling. There is one AAA server within each network, which is located close to the ENs to help delivering secured services to the MNs. The dotted line shows the connection between AAA server and other entity in the network. We also assume that one gateway is located in each access network as an interface with the

This research has been funded by the Industrial Companies who are Members of Mobile VCE, with additional financial support from the UK Government's Technology Strategy Board (Previously DTI).

external IP network. The home network, with home agent (HA) and AAA server, needs to be involved when the information from the home domain is required.

III. SECURITY THREATS, REQUIREMENTS AND OVERVIEW OF THE SOLUTIONS

A. General Security Threats

As defined in [2], network security threats are typically divided into passive and active attacks, which are then subdivided into other types of threats. Based on the framework presented before, we are aiming to solve the following threats:

1) Eavesdropping

The adversary may monitor transmissions for message content at the network level. For example, when a MN is communicating with a correspondent node (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.

2) Masquerading

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

3) 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 the binding update (BU), if they are not properly secured.

4) 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 BUs in a path to book out all the available resources so that the path will run out of resources for any legitimate requests.

B. Specific Security Requirements

Based on the general security threats, a specific set of security requirements for ubiquitous services are derived.

1) 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.

2) Authentication

Authentication is the process of verifying an identity claimed by or for a system entity. The MN needs to be authenticated for the services it requests, such as the handover.

3) Protection of the Handover Signalling

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

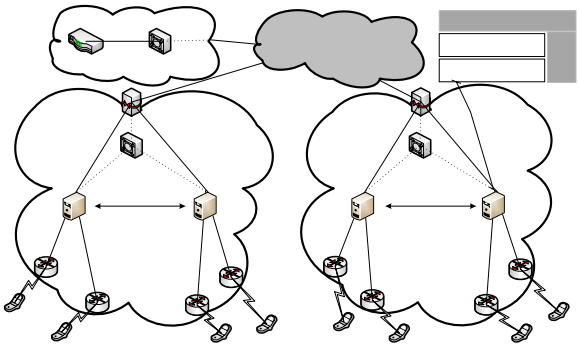


Figure 2. The architectural framework

4) 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 BU to make sure it is not an adversary trying to reserve the resources.

5) Support 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 MM is required.

C. Overview of the Proposed Solutions

The solutions are provided to accomplish the security requirements, namely the authenticated access control scheme and the secured handover process mechanism. The authenticated access control scheme provides MN the authenticated and authorized network access. It prevents unauthorized use of the network resources, such as an adversary accessing the network by masquerading as a legitimate user. Also, authentication and registration are completed in one sequential signalling, which integrates security with MM. The secured handover process mechanism authenticates the MN before the handover and provides the MN secured handover by securing signalling involved, such as BUs.

IV. BACKGROUND ON THE MOBILITY PROTOCOLS

Several mechanisms, such as Hierarchical Mobile IPv6 (HMIPv6) and Fast Handovers for Mobile IPv6 (FMIPv6), have been proposed to reduce the handover latency and the packets loss in Mobile IPv6 (MIPv6) [3]. We assume HMIPv6 as the default mobility agent protocol. FMIPv6 is also used to enhance the fast handovers between different ENs domains.

A. Hierarchical Mobile IPv6 (HMIPv6)

It is anticipated that a few protocols will be widely deployed to enhance MIPv6 with mechanisms for faster handovers [4] [5]. HMIPv6 is one of these proposals. The

main idea of HMIPv6 is to introduce Mobility Anchor Points (MAPs). MAPs 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 scheme like HMIPv6 is to limit the signalling messages locally within the region. That is due to the fact that BUs are sent from MN directly to MAP rather than HA, meaning that MN's exact position is hidden from outer region. 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 "Care-of-Addresses" (CoA). The MN registers the obtained address from its serving AR with the 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 know the MAP and the incoming packets are addressed to the MAP as well. Then, MAP, according to its binding table distributes the packets among the visiting MNs of its domain [6]. Fig. 3 illustrates an example of the use of MAP in a visited network.

B. Fast Handover for Inter enhanced nodes Domains

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 previous AR (PAR) first. Then they are tunnelled to the new AR (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 [3].

With HMIPv6 as the default mobility protocol, EN also plays the role of MAP. HMIPv6 and FMIPv6 are integrated here to further enhance the fast handover. To achieve the integration, ENs need to have prior knowledge of the surrounding ENs and the location of MN. For example, the MN's new location needs to be temporarily registered with the previous EN (PEN). This can be done by the fast handover registration. When a MN moves into a new EN (NEN) domain, the MN obtains a new RCoA and sends a BU to the PEN requesting it to forward packets to the MN's new RCoA. Due to the intelligence, the PEN can be configured to forward packets to the NEN. And the packets finally arrive at the LCoA associated with the AR that is geographically adjacent to AR on the boundary of the PEN domain. This will allow for a smooth inter-EN handover as it allows the MN to continue to receive packets while updating its HA and, potentially, CN.

Fig. 4 shows the signalling involved in inter-EN domains fast handover. Depending on whether a Fast Binding Acknowledgement (FBAck) is received or not on the previous link, there are two modes of operations, namely the predictive mode and the reactive mode. In the predictive mode, after the information for a potential handover is exchanged between MN and AR, the handover is triggered. The MN initiates a Fast Binding Update (FBU) to the PEN, instructing it to redirect its traffic towards the NEN. The PEN and NEN also exchange information and negotiate with each other regarding

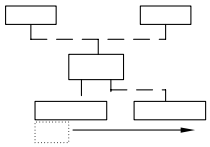


Figure 3. Hierarchical Mobile IPv6 domain [4]

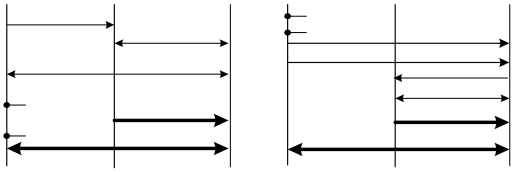


Figure 4. Fast handovers for the inter-EN domains

the MN's handover. The PEN then sends a FBAck message to both of the MN and the NEN as the response to FBU. Afterwards, the packets addressed to MN can be tunnelled from the PEN to the NEN. After the registration is finished, the packets can be delivered between the MN and the NEN as usual as in HMIPv6 specification. The reactive mode operates in a similar way with FBAck received in NEN's link, as shown in Fig.4.

V. SOLUTIONS

A. The Authenticated Access Control Scheme

The method to provide authenticated access for IPv6 supported mobility was proposed in [7]. A similar concept with a few modifications is applied here in our framework. HMIPv6 is used here as the default mobility protocol and the EN has the functionalities of MAP.

1) Overview of the Mechanism

Fig.5 shows the mechanism to integrate fast handovers with the authenticated and authorized access. The AAA servers are located in both of the visited network and the home network. Also, EN acts as the AAA client, which is connected to the AAA foreign server (AAAF). In HMIPv6, the MN must perform the BU to MAP for each RCoA before registration with its HA. The MN may also send a BU to its current CNs. Therefore, it takes three round-trip-times (RTTs) to finish registrations. As illustrated in Fig.5, we integrate the security messages with the BUs, including the BUs to EN and to HA, in order to reduce the RTTs involved in the registration and authentication processes.

The MN first sends the security combined BUs, which include the BUs to both of the EN and HA together with the authentication request, to the EN. The EN initiates an AAA request including the BU (only the BU to HA) to AAAF, which then forwards the request to AAA server in the home domain (AAAH). With the help of HA, the authentication request can be processed locally by AAAH. At the same time, the BU is sent over to the HA by AAAH. Then, the AAAH forwards the security combined binding acknowledgement (BA), which includes the AAA response and the BA from HA,

to the AAAF. The EN then decides whether the MN can be granted the network access, and sends the BAs, including the BAs from EN and HA, over to the MN. The MN registers with its current CN afterwards, if necessary.

The EN plays an essential role in this procedure in terms of controlling both of the registration signalling and the authenticated network access. Also, the RTTs resulted from registrations are reduced by performing two BUs in one sequential process.

2) Details on the Signalling

Fig.6 shows the details on authenticated network access signalling. The common Challenge/Response authentication method for MIPv4 defined in [8] is applied here. The EN provides MN with a challenge on behalf of the HA through an extension to a Router Advertisement message (RA). The MN hashes the challenge with a pre-shared secret key with the home network, and sends the challenge together with the hashed result over to the home network via the AAA infrastructure and waits for the response from the home domain.

Since AAAH can perform the registration with HA on behalf of the MN, AAAH constructs an alternative BU (BU_alt) message that can result in the same registration by MN's BU to the HA (BU_ha) would give. The AAAH can also reconstruct a BA from the HA (BA_ha) message from the alternative BA (BA_alt) in a similar way.

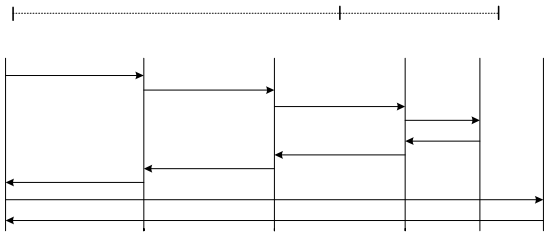


Figure 5. Integration of fast handovers with authenticated and authorized access control

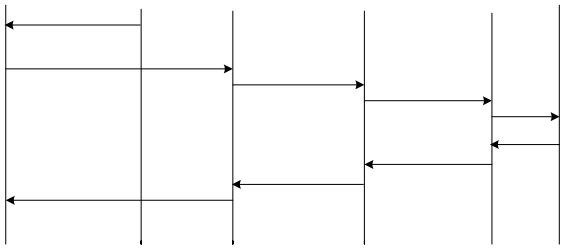


Figure 6. signalling for the authenticated access control scheme

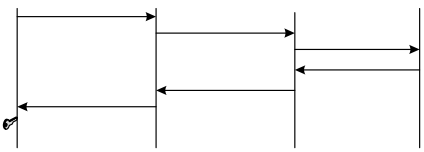


Figure 7. Overview of the key generation procedures

It should be noted that some extensions need to be made on the HMIPv6 messages in order to achieve the sequential registration and authentication. For example, the challenge for each EN needs to be delivered to MNs through the option of the RA message. The messages transmitted between EN and AAAH, including the AAA messages, BU and BA, are all wrapped into the attribute-value-pairs (AVPs) defined for the DIAMETER MIPv6 application in [9] and delivered through the AAA infrastructure. The information transmitted between MN and EN is delivered like a BU to the EN (BU_en) message with the additional information appended in the message options.

B. The Secured Handover Process Mechanism

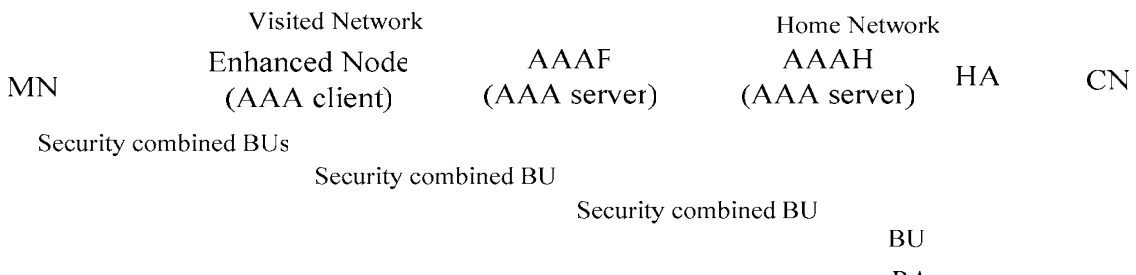
It was proposed in [10] a key management protocol to generate handover keys to secure FMIPv6 signalling. With some modifications and extensions, this method is applicable to other protocols such as HMIPv6. We propose a similar mechanism to secure the handover process for our framework. The secured handover process mechanism 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). The secured handover process includes two procedures: key generation and securing handover messages.

1) Overview of the Key Generation Procedures

Fig. 7 shows the basic key generation procedures. The handover key server (HKS), which cooperates with the MN to generate a HK, is collocated with the AAAF server. The MN, upon attaching to an AR, sends a handover key request (HKReq.) message to the AR. After validating the MN's CoA, AR forwards the HKReq. message to EN. The EN then initiates an AAA request encapsulating the payloads of HKReq. message. After successful authentication and authorization using the Message Authentication Code (MAC) carried in the AAA request, the HKS generates the HK and sends an AAA response message over to the EN. Keying materials and HK are included in this message. The EN decrypts the HK and forwards the HK with the keying information to the AR in a handover key response (HKResp.) message. After receiving the keying materials from AR, the MN then generates the HK.

2) Details of Key Generation Signalling

To expand the messages shown in Fig.7, the detailed signallings are illustrated in Fig.8. We assume that MN and HKS share a pre-shared key (PSK), which is used to generate the HK. The HKReq. message includes the MN's CoA, a nonce generated by MN (N1) and the pseudo random function (PRF) algorithm that MN chooses to use for key generation. Also, MN includes a MAC of the message fields in a MN-HKS MAC option. The value of the MN-HKS MAC is calculated using a handover integrity key (HIK), which is the key derived from the PSK and shared between MN and HKS. Therefore, by validating the MN-HKS MAC, HKS can authenticate the MN and perform authorization for the handoffs before deriving a unique and fresh session key (HK). After successful authentication and authorization, the



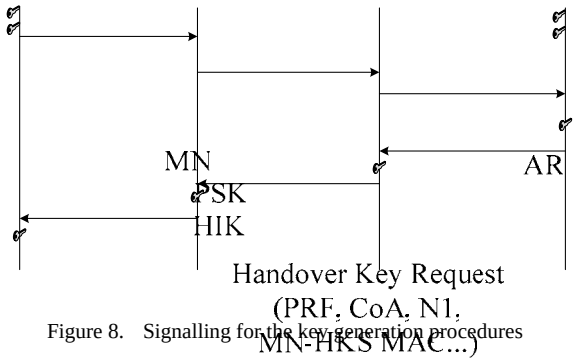


Figure 8. Signalling for the key generation procedures

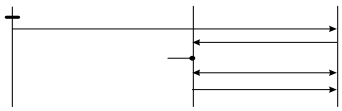


Figure 9. The use of handover key in reactive mode of the fast handovers

HKS sends an AAA response message, including the MN-HKS MAC, a nonce generated by HKS (N2), and the HK. Upon receiving the AAA response, EN decrypts the HK and initiates a HKResp. message, including the keying information from HKS. After receiving a successful response message, the AR stores the HK received from the EN and generates a MN-AR MAC option, which is calculated using the HK. The AR then sends the keying materials with the MN-AR MAC over to MN. Using the keying materials obtained, the MN derives the HK and validates the MN-AR MAC using that.

3) Secure the Handover using the Handover Key

a) Intra Enhanced Node Domain Handover

In the key generation procedure, the MN has already been authenticated and authorized to perform the handover. In the intra EN domain handover, the registration messages are localised within the EN domain, which means in the route of MN-AR-EN. Therefore, when the MN moves between ARs, the BU and BA can be secured using the HK between the MN and the AR pair (or even the MN and the EN pair).

b) Inter Enhanced Nodes Domains Handover

The fast handover signallings as described in section IV B, are secured by HK. In predictive mode of the fast handovers, HK is simply used to secure the FBU and the FBAck. Fig.9 shows how to use the HK to secure the fast inter ENs domains handover in reactive mode. After sending out the Unsolicited Neighbor Advertisement (UNA) message, the MN sends FBU with the HK over to NEN. The NEN then forwards the (FBU, HK) pair to PEN. With the HK formerly generated, the PEN can validate FBU. The HK can also be used in a similar way to secure the QoS-conditionalised BUs.

VI. CONCLUSION

A number of enhancements for MIPv6 are proposed to reduce the handover latency and packet loss rate, such as HMIPv6, FMIPv6 and the combination of both referred to as FHMIPv6, etc. Compared to these protocols, the introduction of ENs in our architecture has the advantage of regulating traffic flow to avoid network bottlenecks, which solves the problem of depending on a single MAP for all users of the domain in HMIPv6. Compared to FMIPv6, the handover latency and packet loss rate can also be further reduced due to the intelligence of ENs. Also, the EN provides an anchor point as part of the AAA hierarchy for the security signalling, which means the security functionalities can be centrally administrated. The EN also provides compatibility with QoS, which integrates security with QoS in a common framework to minimize the negative cross issues. The focal point of this paper is to provide two security solutions for the EN based infrastructure. The authenticated access control scheme aims at authenticating and authorizing the MN when it crosses the networks, while the secured handover process mechanism provides the MN secured micro-mobility and macro-mobility handoffs within one access network. Simulations by OPNET will be carried out to evaluate the efficiency of the solutions.

ACKNOWLEDGMENT

The work reported in this paper has formed part of the Ubiquitous Services Core Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com. Fully detailed technical reports on this research are available to Industrial Members of Mobile VCE.

REFERENCES

[1] Mobile VCE members, “Removing the barriers to ubiquitous services,” Mobile VCE Document, 2003.

[2] T.Karygiannis and L.Owens, “Wireless network security: 802.11, Bluetooth and handheld devices,” National institute of standards and technology special publication 800-48, November 2002.

[3] Jaehwoon Lee and Sanghyun Ahn, “I-FHMIPv6: a novel FMIPv6 and HMIPv6 integration mechanism,” Internet draft: draft-jaehwoon-mipshop-ifhmipv6-01.txt, IETF, June 2006.

[4] H.Soliman, C.Castelluccia, K.ElMalki and L.Bellier, “Hierarchical Mobile IPv6 mobility management,” Internet draft: draft-ietf-mipshop-4140bis-00.txt, IETF, March 2007.

[5] Rajeev Koodli, “Fast handovers for Mobile IPv6,” Internet draft: draft-ietf-mipshop-fmipv6-rfc4068bis-02.txt, IETF, July 2007.

[6] Moloud Mousavi and Alejandro Quintero, “Selection mechanism in Hierarchical Mobile IP,” IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMobapos), pp. 321 – 328, June 2006.

[7] Paal Engelstad, Thomas Haslestad and Frederic Paint, “Authenticated access for IPv6 supported mobility,” Proceedings of the eighth IEEE International Symposium on Computers and Communication (ISCC’03), vol. 1, pp. 569-575, 2003.

[8] C.Perkins and P.Calhoun, “Mobile IPv4 challenge/response extensions,” RFC 3012, IETF, November 2000.

[9] J.Korhonen, J.Bournelle, H.Tschofenig, C.Perkins and K.Chowdhury, “DIAMETER Mobile IPv6: support for network access server to Diameter server interaction,” Internet Draft: draft-ietf-dime-mip6-integrated-08.txt, IETF, February 2008.

[10] V.Narayanan, N.Venkitaraman, H.Tschofenig, G.Giaretta and J.Bournelle, “Establishing handover keys using shared keys,” Internet draft: draft-vidya-mipshop-handover-keys-aaa-04.txt, IETF, March 2007.