An Integrated QoS, Security and Mobility Framework for Delivering Ubiquitous Services Across All IP-based Networks

Yingli Sheng, Haitham Cruickshank
Centre for Communication Systems Research (CCSR)
The University of Surrey
Guildford, Surrey, the United Kingdom

A. Dev Pragad, Paul Pangalos, A. Hamid Aghvami
Centre for Telecommunications Research
King's College London
London, the United Kingdom

***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. One of the important challenges is to integrate Quality of Service (QoS), security and mobility support in heterogeneous networks. To facilitate the interworking of these mechanisms we propose the concept of Enhanced Node (EN) in this paper. The EN is an intelligent entity with a network sub-layer, which integrates QoS, security and Mobility Management（MM）. ENs are located in the access network and they communicate with each other via signalling. In this paper, the functionalities of the ENs are described and the framework with ENs to integrate QoS, security and MM in IP-based networks is presented. The mechanisms to provide the authenticated and authorized access control and to enhance the secured QoS combined fast handovers are also proposed.**

Keywords-QoS; Security; Mobility Management; Enhanced Node; AAA

I. INTRODUCTION

The paper is based on the Ubiquitous Services MVCE Core 4 project, which is working towards accelerating the commercialisation of ubiquitous services by removing the barriers to deployment and adoption from the network perspective. The key barrier to accessing ubiquitous services arises from the need to manage delivery of multiple services within different Quality of Service (QoS) environments through multiple heterogeneous networks. This heterogeneity makes co-operation among them a complex issue. The solution proposed in this paper is to design a common network support sub-layer to integrate QoS, security and mobility functions efficiently. The sub-layer consists of elements of QoS, security and mobility with radio resource management (RRM) hooks. The nodes with the sub-layer support are referred to as 'enhanced nodes' (EN). Within such a framework, translation of QoS, security and mobility mechanisms is required; a common representation of such mechanisms will be used in signalling between ENs to support this (horizontal integration). The ENs, in turn, will operate within the constraints of their access networks, such as the ability to perform authentication and authorization with the help of AAA entities, to perform resource management, to control routing and traffic flow with the aim of meeting the desired end-to-end performance criteria (vertical integration). Such an approach potentially allows existing telecommunication networks to be enhanced without the additional delays associated with network standardisation through selective upgrades of a limited number of network nodes [1].

II. ARCHITECTURE FOR THE ENHANCED NODE

In this section, the architecture and framework of the ENs describing the components of the framework and their functionalities are presented. The primary functionality of the EN is to gather QoS, security 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 five major components namely: QoS, Security, Mobility Management (MM), RRM and Signalling as shown in Fig.1. 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 [1].

A. Mobility Management

The mobility component of the sub-layer provides the framework to manage the functions relating to MM within access network and across access networks. This entity can function as the Mobility Anchor Point (MAP) of Hierarchical Mobile IPv6 (HMIPv6) but can also enhance the existing MM mechanisms. It does this by providing them with additional information required to take optimal decisions regarding mobility within and more specifically across access networks [1]. The mobility entity will interact with other entities

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).

involved in providing mobility to Mobile Nodes (MN) as shown in Fig. 2.

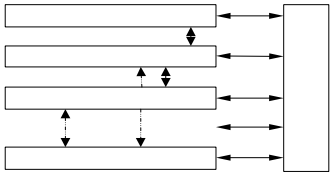

Figure 1. The architecture of the enhanced node

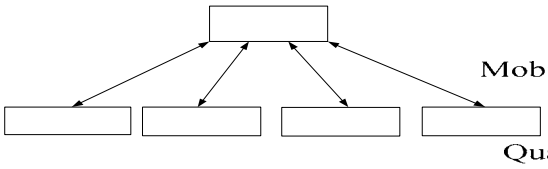

Figure 2. Mobility entity interaction with other entities [1]

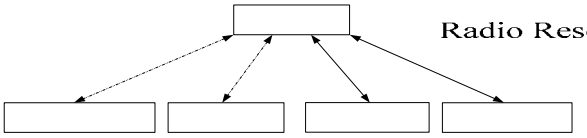

Figure 3. QoS entity interaction with other entities [1]

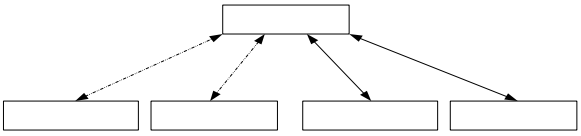

Figure 4. Security entity interaction with other entities

Access Points Access Routers Mobile Nodes Mobility Agents (MAP)

B. *Quality of Service Provisioning*

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. Fig. 3 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 [1].

Enhanced Node (QoS) QoS Routing/Congestion Management Traffic Shaping/ Call Admission Mobile Nodes Resource Manager/ Enhanced Routers

C. *Security*

The security component of the sub-layer plays a crucial role in providing security services within one access network and across heterogeneous networks. Before a MN can enter an access network, it should be authenticated and authorized by certain access control scheme with the help of AAA entities. The EN acts as an AAA client, which is connected to both of the access routers (AR) and the AAA servers. Under this infrastructure, authentication can be performed together with MM signalling. Also, the MN is authenticated for the handover and the handover signalling between the EN and the MN can be secured by handover key. Therefore, the EN, which is also an AAA client, is in charge of the security services throughout the networks, in terms of controlling the authenticated access and the key generation. Fig. 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 by the EN, such as the secured handover and the authenticated access control.

D. *Radio Resource Management*

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 [1].

E. *Signalling*

The signalling entity plays an important part. This entity enables the EN to gather information and share information through signalling other entities. Integration of QoS, security 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 [1].

III. THE BASELINE ARCHITECTURE

The ENs interact with other like nodes present within the access network and across other access networks [2] as shown in the baseline architecture in Fig. 5. In this figure more than one EN is located within each access network and these nodes communicate with each other via signalling. 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 [1].

The aim of this IP network is to deploy QoS, security and MM mechanisms in order to provide enhanced services to users. However these mechanisms have interactions with each

Enhanced Node (Security)

Secured Handover Authenticated Access Access Routers AAA Servers

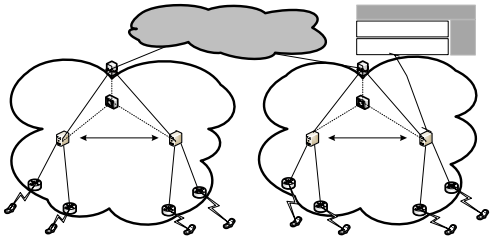

Figure 5. Baseline architecture for the enhanced node

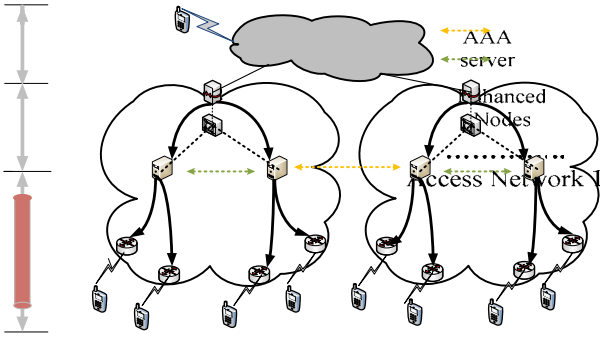

Figure 6. QoS, security and mobility architecture framework

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 QoS and security 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 with the help of AAA servers when the MN moves across access networks. 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.

IV. FRAMEWORK FOR THE COMBINED QOS, SECURITY AND MOBILITY MECHANISMS

Much research has recently been undertaken in proposing and designing QoS, security and MM 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 [3] and MIND [4] 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. The negative cross issues between QoS and security need to be addressed in terms of minimizing the handover latency caused by security mechanisms and securing the QoS signalling if necessary. Although aimed at solving different aspects of network operations, both QoS routing and micro-mobility protocols influence packet forwarding in scoped domains. Hence, applying different QoS routing schemes [5] inside mobile network domains calls for an investigation of the cross issues with micro-mobility protocols [6], [7] and [8]. In [9] it was shown that such cross issues can be so significant that routing decisions between the two mechanisms may contradict resulting in a sudden break of communication between the gateway of the scope domain and the mobile host.

In this section, we define and discuss the framework for the combined QoS, security and mobility mechanisms. The signalling diagrams are used to illustrate the functionality of the ENs as well as emphasize the details of the combined mechanisms. This work considers an IP-based access network, assumes HMIPv6 as the default mobility agent protocol and supports a generic QoS framework able to support both Intserv and Diffserv architectures. The EN is given the role of MAP. The main elements of the architecture are shown in the signalling diagram Fig.6. The gateway is a special purpose router with interfaces between the access network and an external IP network. The ENs are essentially normal mobility agents enhanced by an innovative network support layer. The ENs are responsible for integrating QoS, security and mobility efficiently within the access network. The role of the EN is to minimize the delays involved in reestablishing the QoS after a handover and to help establish the handover keys to secure the handover process. In terms of security, the ENs, acting as the AAA clients which connect to the AAA servers in both of the foreign domain and the home domain, also play an essential role in authenticated access control. The ENs are also assigned the functionality of monitoring the resources used by the existing sessions. Since most of the sessions requiring high QoS and low latency flow through the EN, the EN will be able to perform call admission and also shape the traffic in the access network as well as regulate the QoS. The aim in terms of QoS and mobility is to keep any required signalling within the EN domain [10] and from security point of view to interact with the AAA servers to provide secured services.

A. Authenticated Access Control

Fig.7 shows the signalling involved when security and mobility signalling are coupled to each other. The authenticated and authorized access control needs to be executed before the network access is granted to the MN. The method to provide authenticated access for IPv6 supported mobility was proposed in [11]. Similar concept is applied in our framework. The authentication messages and registration signalling, including the Binding Updates (BU) and Binding Acknowledgements (BA), are combined. Therefore, authentication and registration are completed in one round-

trip-time (RTT).

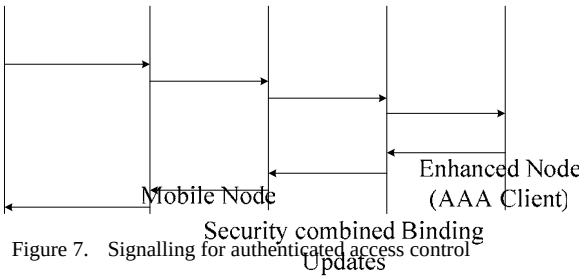

Figure 7. Signalling for authenticated access control

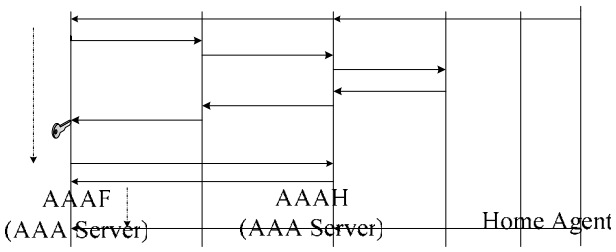

Figure 8. Signalling for intra domain handover

After AR issues a Router Advertisement (RA) message to MN, the MN sends the security combined BUs, which include the BUs to EN and Home Agent (HA) together with authentication request. Upon receiving the combined BUs, the EN, acting as an AAA client, initiates an AAA request and sends the request together with the BU (only the BU to HA) to AAA server in foreign domain, namely AAAF. The AAAF forwards the message to AAA server in home domain, namely AAAH. With the help of HA, the AAA request can be processed locally by AAAH, which initiates an AAA response message as the result. At the same time, the BU is sent to the HA by AAAH. Then, the AAAH forwards the security combined BA, which includes the AAA response and the BA from HA, to AAAF. Using the AAA response received from AAAF, the EN can decide whether the MN can be granted the network access. Then the EN sends the BAs, including the BAs from EN and HA, over to the MN. The EN plays a vital role in this procedure, in terms of controlling both of the registration signalling and the authenticated network access.

B. Intra Domain Handover

Fig. 8 shows the packet flow and the signalling involved when QoS and mobility signalling are coupled to each other. The concept of QoS conditionalised handovers was first introduced in [12]. The concept behind this is to use the same signalling for sending the BU and the QoS request instead of sending two different signalling messages. We use a similar concept. One signalling message to notify the ENs about the update in the location of the MN as well as setting up the new QoS path to the new destination. As the number of MNs increase so does the mobility rate. As a result of this increase, the signalling overhead will be very large. This proposed solution halves the signalling overhead and at the same time halves the QoS based handover time for the MN [10].

From security point of view, the secured handover scheme that generates the handover key (HK) to protect the handover process is clearly illustrated in Fig. 8 as well. It was proposed in [13] a key management method to secure the Fast Handovers for Mobile IPv6 (FMIPV6) signalling. With some modifications and extensions, the method can be applied here. The MN is authenticated for the handover. The key generation procedure takes place before the handover, therefore, the HK can be used to protect the handover signalling and the QoS signalling involved if it is necessary.

A MN, upon attaching to an AR, sends a handover key request (HKReq.) message, which includes a set of keying materials, to the AR. The AR then forwards the request to EN. The EN, as an AAA client, then initiates an AAA request encapsulating the HKReq. information and sends it to handover key server (HKS), which is also the AAAF server. By validating the Message Authentication Code (MAC) in the HKReq. message, the HKS can authenticate the MN. Also, a unique and fresh session key can be derived using the keying materials at the same time. The HKS then returns an AAA response message to the EN. The keying materials and the HK are encapsulated in this AAA response message. Upon receiving the response from the HKS, the EN then decrypts the HK and sends a handover key response (HKResp.) message to the AR. The HKResp. message includes the HK and the keying information. After the AR receives the HKResp. message, it stores the HK and sends the response over to the MN, including the keying materials that the MN requires to generate the HK.

The MN is authenticated before performing handover and requesting resource so that the adversary can not book out all the resources leading to a Denial-of-Service (DoS) attack. After the HK is finally generated at the MN, it can be used to secure the signalling involved in the handover process afterwards, such as the BU or even the QoS combined BU.

C. Inter Domains Handover

One of the major areas where work still needs to be done is in the process of inter mobility agents handovers. During a handover between mobility agents, the location update needs to be sent to the correspondent node (CN) and the HA. During this, the regional care of address (RCoA) obtained from the mobility agent changes and the packets that the CN transmits to the MN need to be readdressed to the new RCoA of the new mobility agent. In the proposed architecture the handover will occur between ENs [10].

Fig.9 shows the signalling for inter ENs handover scenario with combined QoS and mobility update. During the handover period the packets arriving at EN1 are stored and redirected to EN2 where the MN is currently connected [10]. This process is clearly illustrated in Fig. 10. The MN associates itself with a new EN and obtains a new RCoA. In turn the MN then performs a global location update to its CN which could result in large delays and packet loss. During this handover period

packets generated by CN will still be arriving at the MN's old location (EN1). To minimize the loss in packets, the EN1 redirects the packets it receives from the CN to the new location of the MN (EN2). In turn EN2 tunnels these packets to the MN. To make this possible the address of EN2 needs to be temporarily registered with the EN1. Therefore the maximum delay experienced is the time it takes for the MN to receive a new IP address (from EN2) and notify EN1 about its new location. This delay can be minimized if the ENs have prior knowledge of the surrounding ENs as well as location information of the MN. For example, by using fast handovers

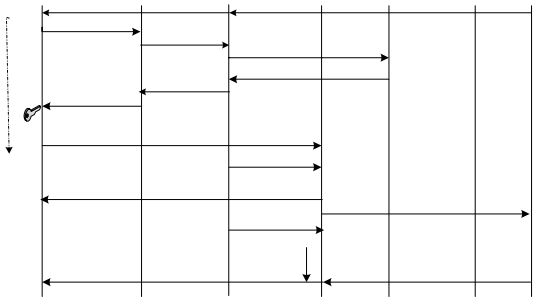

Figure 9. Signalling for inter-EN domains handover

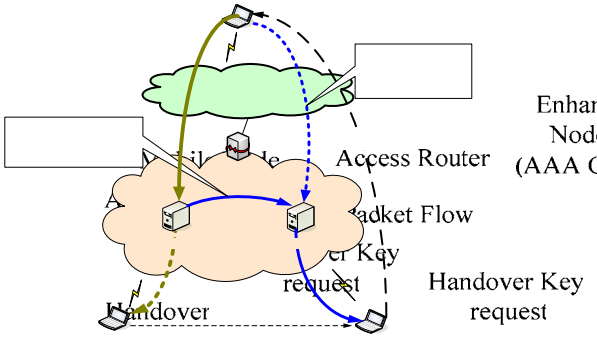

Figure 10. Packet redirection during inter-EN domains handover [10]

EN1 can be notified about the new location of the MN (EN2 and local address) before the handover takes place [10].

Fig.9 also shows the signalling for handover key generation procedures. The process is similar as described in the Intra domain handover. The HK can be used to secure the signalling in the fast handovers, such as fast BU (FBU). MN first informs EN2 of the attachment and also confirms the use of new CoA. With HK generated, the MN then sends a FBU message with the HK over to EN2. The EN2 forwards the FBU with the HK to EN1. With the HK previously generated, EN1 can validate the FBU and authenticate the MN. Then, the EN1 can send a fast BA (FBA) to EN2 to finish the fast handover registration. The HK can also be used in a similar way to secure the QoS combined BU to make the QoS message resilient to DoS attack. And MN is authenticated before the QoS context transfer takes place. This ensures the QoS context is transferred to the EN2 as it claimed but not an adversary, which prevents the masquerading attack.

V. CONCLUSION

The proposed scheme with ENs can integrate QoS, security and MM rather than managing them independently in IP-based access networks in order to deliver ubiquitous services efficiently and securely. With the integration approach, the negative cross issues between QoS, security and MM can be minimized and the network performance can be enhanced in terms of reducing the handover latency, network congestion, load balancing and packet loss probability. Based on the baseline framework, the security mechanisms are presented to provide mobile user network access control, and also to enhance secured QoS combined fast handovers. The security framework can result in better resilience to security attacks, amongst other benefits. The quantitative benefits of the proposed framework are currently being modelled and quantified by the Performance Evaluation Process Algebra (PEPA) [14]. PEPA is a mathematical tool which models and reasons about the structure and behavior of systems.

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] Dev Pragad, Yingli Sheng, Hao Wang, George Kamel and Paul Fergus, "Deliverable U2.2: Architecture for network support sub-layer," Mobile VCE Core 4 Research Programme: Ubiquitous Services, October 2006.

[2] Dev Pragad, "Mobility and QoS architecture for the network support sub-layer," Mobile VCE Core 4 Research Programme: Ubiquitous Services, ICR 2.1.2, September 2006.

[3] IST-1999-10050 BRAIN Deliverable D2.2, "BRAIN architecture specifications & models, BRAIN functionalities and protocol specifications," March 2001.

[4] IST-2000-28584 MIND Deliverable D2.2, "MIND protocols & mechanisms specifications, simulation & validation," November 2002.

[5] G.Apostolopoulos, et al., "QoS routing mechanism and OSPF extensions," RFC 2676, IETF, August 1999.

[6] S.Pack and Y.Choi, "A study on performance of hierarchical Mobile IPv6 in IP-based cellular networks," IEICE Transactions on Communications, Vol. E87-B, No. 3, March 2004.

[7] Qian Zhang, Chuanxiong Guo, Zihua Guo and Wenwu Zhu, "Efficient mobility management for vertical handoff between WWAN and WLAN," IEEE Communications Magazine, vol. 41, issue 11, pp. 102–108, November 2003.

[8] Varma V.K., et al., "Mobility management in integrated UMTS/WLAN networks," IEEE International Conference on Communications, vol. 2, pp. 1048-1053, May 2003.

[9] V.Friderikos, A.Mihailovic and A.H.Aghvami, "Analysis of cross issues between QoS routing and mobility protocols," IEE Proceedings Communications, vol. 151, No. 3, June 2004.

[10] Dev Pragad, et al., "Deliverable U2.3: mechanisms for combining mobility, Quality of Service and security," Mobile VCE Core 4 Research Programme: Ubiquitous Services, April 2007.

[11] 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.

[12] X.Fu, H.Karl and C.Kappler, "QoS-conditionalized handoff for Mobile IPv6," in Networking 2002, LNCS, vol. 2345, pp. 721–730, 2002.

[13] 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.

[14] Jane Hillston, A compositional approach to performance modelling, Cambridge University Press, 1996.