A Context Transfer Model for Secure Handover in WiMAX/LTE Integrated Networks

E. Prince Edward, Sri Krishna Polytechnic College, Coimbatore, India

ABSTRACT

One of the recent research issues in IP Multimedia Subsystem (IMS) based heterogeneous internetworking environment is to provide secure handover when a mobile node (MN) moves between different access networks. Various security schemes are available in literature but most of the schemes provide security but degrades the Quality of Service (QoS). The objective of this work is to provide secure and efficient handover in an IMS based Worldwide Interoperability for Microwave access (WiMAX)/Long Term Evolution (LTE) integrated networks by using the proposed Secure Context Transfer Model (SCTM). New Session Initiation Protocol (SIP) messages are introduced in the proposed SCTM for transferring the context securely from old Proxy-Call session control function (P-CSCF) server to new P-CSCF server during handover. SCTM is verified using NS-2 simulator and analyzed based on Queuing theory. The results show that when compared with previous approaches, SCTM shows an improvement of 23% in terms of handover delay and packet loss providing security and guaranteed QoS to mobile users.

Keywords: Integrated Wireless Networks, LTE, Secure Context Transfer Model, Vertical Handover, WiMAX

INTRODUCTION

The next generation wireless networks strive to efficiently integrate existing multiple heterogeneous networks and make modification of protocol and signaling schemes as few as possible instead of developing an all new network. This can be achieved by integrating the different wireless access networks such as IEEE 802.11, IEEE 802.16, LTE, GPRS, 3G and UMTS. One of the most prominent wireless technologies today is IEEE 802.11 wireless LAN also called as Wireless Fidelity (WiFi). Based on IEEE 802.11 standard personal devices like Laptop, mobile devices connect to the Internet in a limited range with an access point (AP). 3G technology offers universal network access but the access rate is very limited. IEEE 802.16 also called as WiMAX can provide high speed internet access in wide area. The new emerging wireless technologies are WiMAX and LTE. Both are relatively new but very promising standard for wireless communication. To put it in brief they provide the speed of WiFi and the coverage of 4G. The integration of WiMAX and LTE networks can combine their best features to provide a complete wireless scheme for delivering high speed Internet access to businesses, homes and hot mobile nodes. Long Term Evolution is a 4G mobile technology...
developed by a standards-developing body called the Third Generation Partnership Project (3GPP). 4G LTE is a much advanced technology than the existing mobile technology which aims to provide mobile users with features like VoIP, high quality video conferencing, video messaging etc. Nevertheless such handover preparations have not been mentioned in the 4G LTE systems standards. Hence an absolute handover scheme with security is in need to be developed for LTE network.

The IP Multimedia Subsystem (IMS) was originally designed by the 3GPP for delivering multimedia services over Internet Protocol (IP) networks (3GPP IMS). However, since the IMS networks are still in a development stage, there are unsolved open issues such as QoS, efficient service provisioning and providing data security during handovers. In general, security procedures make the handover process more complex in a wireless and mobile environment (Bilal et al., 2007). Authentication and Authorization are the most vital parameters for a roaming user, but the bandwidth utilization is increased during the handover phase (Karopoulos et al., 2006). Hence in heterogeneous networks it is very important to maintain trade-off between security and QoS during handover. In order to meet the requirements of secure and efficient vertical handover process, proper solutions must be formulated for heterogeneous networks. This motivation has enabled the author to design SCTM to provide secure and efficient handover in an IMS based WiMAX/LTE heterogeneous networks.

RELATED WORKS

Most of the existing security mechanisms available in literature add complexity and overhead to handover management. Hence it is very important to maintain trade-off between security and QoS during handover. The tradeoff among these two parameters will increase more when service provider is different from network provider. In such cases, it is essential for a roaming user to get authenticated both from network provider as well as service provider. Here, AAA protocol is used for authentication, which is more costly. Furthermore the distance from the home network and visited network is higher which adds handover delay (Faraz et al., 2007). MPA (Media-Independent Pre-Authentication) (dutta et al., 2008) is another effective authentication methodology used in handover. MPA mechanism does not provide security while exchanging messages during handover and more packets are lost if handover takes place before the completion of binding update. But it also adds latency during the handover process. The Extensible Authentication Protocol (EAP) is a client server protocol which uses the authentication server to implement authentication process (Gaabab et al., 2007). (Reem et al. 2014) have utilized EAP Authentication and Key Agreement (EAP-AKA) for IMS based WiMAX/LTE secure handover. But EAP-AKA process involves various exchange of messages and repeated execution every time when a handover occurs. IPSec is one of the techniques used for data security, for providing security to those messages that run over IP protocols, i.e., IPv6. For real-time services, such as voice and video, the SIP (Rosenberg et al., 2002) is becoming the leading signaling protocol in IP networks and has already been accepted as the signaling standard by IETF and 3GPP. SIP is used as the signaling protocol for IMS networks. Furthermore SIP has the provision for encapsulating the IP Sec packets within the SIP request and Response message structure.

A vertical handover (VHO) occurs when a mobile user changes his point of attachment from one type of wireless access network to another during an active communication session. When a Mobile Node (MN) performs vertical handover during an ongoing session in a IMS heterogeneous environment for e.g., moving from WiMAX to LTE network, it has to re-register its obtained new IP address at the IMS network for re-authorization and setting up a new session via the LTE network. The delay incurred during the re-authorization process is called the ‘IMS re-authorization delay’. The IMS re-authorization process for each IMS network would consume substantial network
Collaborative Access to Ancient Documents: Towards a Distributed Comparison of Pre-Processing Approaches
www.igi-global.com/article/collaborative-access-ancient-documents/69532?camid=4v1a

A Proposal for Enhancing the Mobility Management in the Future 3GPP Architectures
www.igi-global.com/article/proposal-enhancing-mobility-management-future/55085?camid=4v1a