3rd International Graduate Conference on Engineering, Science and Humanities (IGCESH)
School of Graduate Studies Universiti Teknologi Malaysia
2 – 4 November 2010

Security Zone and Key Derivation Management in Centralized Security Control in Wimax Multihop Relay System

Adnan Shahid Khan [1], N. Fisal [1], N.N.M.I. Ma'arof [1], Fath.E.I. Khalifa [1], M. Abbas [2], Hashim E. A. Elshafie[1]

Email: adnan.ucit@gmail.com, sheila@fke.utm.my, nnazirah@fkegraduate.utm.my, fathi_sml@fkegraduate.utm.my, mazlan.abbas@mimos.my, hashim530@hotmail.com[1]
[1] UTM-MIMOS Center of Excellence, Faculty of Electrical Engi ng, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia.
[2] Wireless Communication Cluster, MIMOS Berhad, Technology Park Malaysia.

Abstract

A wireless internet services are rapidly expanding and improving, it's important to provide users with not only high speed and high quality wireless service but also secured. Mesh networking support was added for improved coverage and throughput. A WiMAX mesh network not only increases the wireless coverage but a so provides features such as lower backhaul deployment cost, easy setup and deployment, robustness and re-configurability, which make it one of the indispensabl technologies in next generation wireless network. In order to operate efficiently, communication must be scheduled either by a distributed, centralized or hybrid algorithms. A WiMAX network usually operates in a highly dynamic and open environment therefore it is known to be more vulnerable to security holes. In this paper, we give a detailed overview of privacy key management protocol (PKM) and key derivation management in centralized security zone control in a multihop relay system. Here we also try to discuss the trade offs of centralized and distributed security zones and key management in multihop relay system.

1.0 Introduction

With centralized security control residing in the MR-BS in the multihop relay system, the security association is established between MS/RS and MR-BS without the involvement from the intermediate RS. The RS does not try to decrypt the user data or authenticate the MAC management message it receives from the MS, but simply relays it. All the MS-related keys are stored and maintained at the MS and MR-BS, and RS does not have any key information associated with the MS. With centralized security control residing in the MR-BS in the multihop relay system, the security association is established between RS and MR-BS without the involvement from the intermediate RS. AK security context is shared and maintained at the particular RS MR-BS, and the intermediate RS does not have this information. The intermediate RS authenticates management messages it receives from other RSs using relay-specific shared keys. Similar to other MAC management messages, all the PKM messages are exchanged between MS/RS and MR-BS. For the PKM messages that are not protected by the message authentication code from the MS/RS (termed as non-authenticated PKM messages, e.g., Auth Request, Auth Reply, PKMv2 RSA-Request, PKMv2 RSA-Reply), the following procedure may be applied. For all the other cases, the access RS and the intermediate RSs just simply relay the PKM messages. Upon receiving a non-authenticated PKM message, the access RS may add the HMAC/CMAC tuple based on the SA established between itself and the MR-BS into the message. Upon receiving a non-authenticated PKM message with the presence of HMAC/CMAC tuple, the MR-BS authenticates the message based on the shared SA between itself and the access RS. When the MR-BS generates a non-authenticated PKM message to the MS, it may add the HMAC/ CMAC tuple based on the SA established between itself and the access RS. Upon receiving a non-authenticated PKM message with the presence of HMAC/CMAC tuple, the access RS authenticates the message based on the SA between itself and MR-BS. If the message is valid, it then removes the HMAC/CMAC tuple, and then sends the PKM message to the MS.

Distributed security control in a multihop relay system When an access RS is operating in distributed security mode, the authentication key established betw SS and MR-BS is distributed to this RS. During the registration process, an RS can be configured to operate in distributed security mode based on its capability. An RS operating in this mode relays initial PKM messages between the MR-BS and SS/ subordinate RS. When the MSK for a subordinate RS/SS is established, the MR-BS shall securely transfer the relevant Authorization Key