Jurnal Teknologi

Full paper

# Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks

Adnan Shahid Khan*, Halikul lenando, Johari Abdullah, Norsheila Fisal

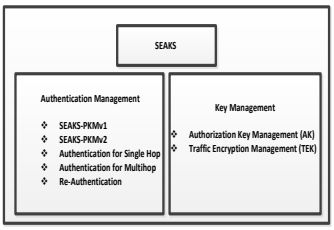
*Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak*

*Corresponding author: skadnan@fit.unimas.my

**Article history**

Received: 14 July 2014
Received in revised form:
16 Oktober 2014
Accepted: 1 February 2015

**Graphical Abstract**




**Abstract**

Mobile Multihop Relay (MMR) network is one of the emerging technologies, especially LTE-Advanced, WiMAX and the Smart grid communications. Ensuring security is one of the most imperative and challenging issues in MMR networks. Privacy Key Management (PKM) protocol is proposed to ensure the security measures in MMR networks. However, the protocol still faces several security threats, specifically Denial of Service (DoS), replay attacks, Man in the Middle (MitM) attacks and the interleaving attacks, which is termed as Medium Access Control (MAC) layer attacks. This paper proposed a modified version PKM protocol for both unilateral and mutual authentication, which is termed as Self-organized Efficient Authentication and Key Management Scheme (SEAKS) authentication protocol. This protocol ensures secure end-to-end data transmission using distributed hop-by-hop authentication and localized key management schemes with a very simple and efficient way.

*Keywords*: MMR WiMAX network; security issues; IEEE 802.16; denial of service; hop-by-hop authentication



## 1.0 INTRODUCTION

Introduction of relays to support multi-hopping in Mobile Multihop Relay (MMR) WiMAX networks not only increases the wireless converges but also provides features such as lower backhaul deployment cost, easy setup and high-throughput [1]. Security is essential in wireless technologies to allow rapid adoption and enhance their maturity. Security specifications can mainly be found within the Medium Access Control (MAC) layer, which is called security sublayer. WiMAX has security vulnerabilities, which may create a significant disruption in communication with little effort from the attacker thus could threaten its wide-spread deployment [2]. In the security sublayer of WiMAX, two sets of protocols are provided: an encapsulation protocol for encrypting data across Broadband Wireless Access (BWA), and a PKM protocol for secure distribution of keying materials from the Base Station (BS) to the Subscriber Station (SS) and for enforcing conditional access by the BS. The PKM protocols works in two different versions, i.e. PKMv1 and PKMv2. PKMv1 allows only unilateral authentications, and PKMv2 allows mutual authentications. It also supports periodic re-authentication/re-authorization and key refresh [3]. The PKM's authentication protocol establishes a shared secret Authorization Key (AK) between the SS and the BS. The shared secret is then used to secure subsequent PKM exchanges of Traffic Encryption Keys (TEKs). An SS uses the PKM protocol to obtain authorization and traffic keying material from the BS and to support periodic reauthorization and key refresh. PKM supports two distinct authentication protocol mechanisms that are RSA (Ron Rivest, Adi Shamir and Leonard Adleman) protocol [1], and Extensible Authentication Protocol. This study only focuses on PKM-RSA protocol.

In general, research challenges for MMR WiMAX network arise primarily due to the large number of constraints that must be simultaneously satisfied. One of the major constraints is the lack of physical boundaries that leads towards several attacks, especially DoS, replay attack, MitM attack and interleaving attacks [4-6]. Secondly; authentication overhead is also one of the key constraints. In MMR network, either centralized authentication or distributed authentication can be used. If centralized authentication is used, every multihop node should always be accessible to the authenticator server, therefore, could be overloaded to handle the mutual authentication among all nodes on the network. Hence, each multihop node needs to contact the authentication server whenever authentication is required. This scheme may generate authentication overhead and thus is not suitable for MMR networks where each node keeps moving and wants to authenticate many neighbour's nodes [4, 7, 8]. On the other hand, if distributed authentication is used, it is very difficult to share initial trust information among the relays for mutual authentication. Thirdly, due to lack of trust within the participating relays, an internal attack may occur from the rogue relay stations [9-11]. If this rouge relay station increases thus cause a severe and unbearable loss to the deployment. However, author [9] discussed Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations. This protocol works better for the centralized security mechanism where the scalability is the issue. Author [3] described all the possible attacks and their countermeasure; however, they mainly focused more on mobile WiMAX, thus literature on the modification of PKM protocol for MMR networks is scare. To