

An Improved Authentication Key Management Scheme for Multihop Relay in IEEE 802.16m Networks

Adnan Shahid Khan¹, Norsheila Fisal¹, Mazlina Esa², Sharifa Kamilah¹, Sharifa Hafizah¹, M. Abbas³

¹*UTM-MIMOS Center of Excellence, Faculty of Electrical Engineering*

²*Radio Communication Engineering Department*

Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia.

³*Wireless Communication Cluster, MIMOS Berhad, Technology Park Malaysia*

Abstract:

Relaying and cooperation have re-emerged as important research topic in the wireless communication over the past decade. IEEE 802.16m Multihop relay network is assiduously developing to accomplish high capacity services with large cell coverage. Considerable interest currently exists in the exploitation of Relay based Wimax. This is mainly the result of lower infrastructure cost and high data transfer rates compared to existing 3G. However due to lack of physical boundaries and injection of distributed relays, it is known to be more vulnerable to security holes as a trade off. In this paper we propose a new distributed authentication key scheme for Multihop Relays IEEE 802.16m network service. The propose scheme uses decode and forward relays with localized authentication. The scheme works in distributed authentication to authenticate Subscriber station (SS) and Relay stations (RS) at initial network entry. Our new improved distributed scheme utilizes healthy security issues and the Multihop Relay network application features. Both analysis and performance evaluation shows that our scheme can significantly increases the network throughput and reduce the security holes as well as communication overheads.

Keywords: *Distributed Networks; IEEE 802.16j; Multi-Hop Relay; Key Management; Traffic Encryption Key.*

1. Introduction

Wireless networks have become more and more pervasive due to their many advantages. The IEEE 802.16 standard aims to provide broadband wireless access (BWA) for metropolitan area network (MAN), and is to design for the delivery of last mile BWA is alternative to the cable and DSL. To support BWA, high data transmission is necessary. In March 2006, a new task group IEEE 802.16m was introduced, which attempts to amend current IEEE 802.16e standard just by injections of RSs in between BS and Subscriber Stations (SSs) in order to support multi-hop relay operation in wireless broadband networks. This relays may operate in three possible schemes, depending on how it process the received signals amplify and forward, decode and forward and estimate and forward. As the matter of fact, any relays operate in amplify and forward scheme or transparent mode cannot decode the control information from the Multihop Relay base station (MR-BS). Contrary, Relays operates in decode and forward scheme or non-transparent Access Relays (NT-ARS) must transmit control information by themselves. Here we assume that relays is operating in non-transparent distributed scheduling and security mode, which can show better performance than other RS [2]. At the same coin, wireless networks represent an important example of such scenarios where capturing and forging packets is relatively easy; attacks against such networked system are becoming more complex and powerful. Thus, security is essential in wireless technologies to allow rapid adoption