ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Analysis and Comparison of WiMax Communication using Cryptographic Techniques

Mrs. Shallu Makker[1], Mrs. Vidhu Kiran[2]

JCD College of Engineering, Sirsa, Haryana[1,2]

Abstract: WiMax means Worldwide Interoperability for Microwave Access. It is the wireless technology and enhancement of 802.16 standards. WiMax has many salient advantages suchas: high data rates, quality of service, scalability, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks. In WiMax, security is the major issue for transmission of data from end to end. We discuss the WiMax security mechanisms for authentication, encryption, and availability. Security protocols are essential for secure transmission of data. Throughput and Packet delivery ratio (PDR) can be increased by using security protocols like AES and RSA. In this report, we study the comparative results of different security protocols in terms of Throughput and PDR by applying encryption schemes of RSA and AES.

Keywords: WiMax, Cryptographic Techniques, Packet delivery ratio (PDR), AES, RSA.

1. INTRODUCTION

Worldwide Interoperability of Microwave Access, also known as the IEEE 802.16 protocol, the latest and most renowned standard for wireless networks.
Many enhancements were carried out in this standard with special attention on high quality of service, Security and the use of Scalable OFDMA techniques .Despite of so many advantages that WiMAX provides, security has been considered as the main issue during the design of the protocol.. WiMAX is a new technology; and more prone to threats, risk and vulnerability in real situations. To understand the security aspects of IEEE 802.16 technology, it is required to provide an overview of this standard as a relevant work. A lot of theoretical work has been done on security issues related to WiMAX. The key point of our research paper is that we have not only discussed various security issues theoretically but also simulated them to get better understanding about how to secure WiMAX traffic using modern cipher algorithms like AES and RSA.

From the end user point of view, the primary security concerns are privacy and data integrity. Users need assurance that no one can bug somebody's room on their sessions and that the data sent across the communication link is not altered. This is usually achieved through the use of encryption. From the service provider's point of view, an important security consideration is preventing unauthorized use of the network services. This is usually done using strong authentication and access control methods. The service provider's need to prevent deceptionshould be balanced against the inconvenience that it may inflict on the user. Security is an important consideration in any communications system design but is particularly so in wireless communication systems. In Networking, There are number of security protocols for efficient and reliable communication with no loss of packets and confidentiality of packet delivery. The protocols efficiency and security depends on different parameters such as PDR (packet delivery ratio), Throughput etc. WiMAX encrypts neither the MAC headers nor the MAC management messages, with the purpose to enable various operations of the MAC layer. Therefore, an attacker, as a passive listener of the WiMAX channel, can retrieve valuable information from unencrypted MAC management messages. Spying of management messages may reveal network topology to the eavesdropper, posing a critical threat to SSs as well as the WiMax system.

2. PROTOCOL ARCHITECHTURE

The IEEE 802.16 protocol structure is all in the (PHY) Physical and the (MAC) Medium Access Control layers. The MAC layer can be further classified into three sub layers, the first one is (CS) Service Specific Convergence Sub-layer and the second is (CPS) Common Part Sub-layer and third is the Security Sub layer. Convergence Sub layer is the sub-layer that communicates with upper layers to obtain network data and it transforms these data into MAC Service Data Units (SDUs).

The main MAC functions are such as bandwidth allocation, connection establishment and connection maintenance. The Security Sub-layer functions are such as verification, approval, key establishment, allocation and management. It is also responsible for encryption and decryption of traffic passing from the PHY to the MAC layer and vice versa.

3. OBJECTIVES

3.1 Problem Definition

From the point of view of an end user, the primary security concerns are privacy and data integrity. Users need assurance that no one can eavesdrop on their sessions and that the data sent across the communication link is not tampered.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

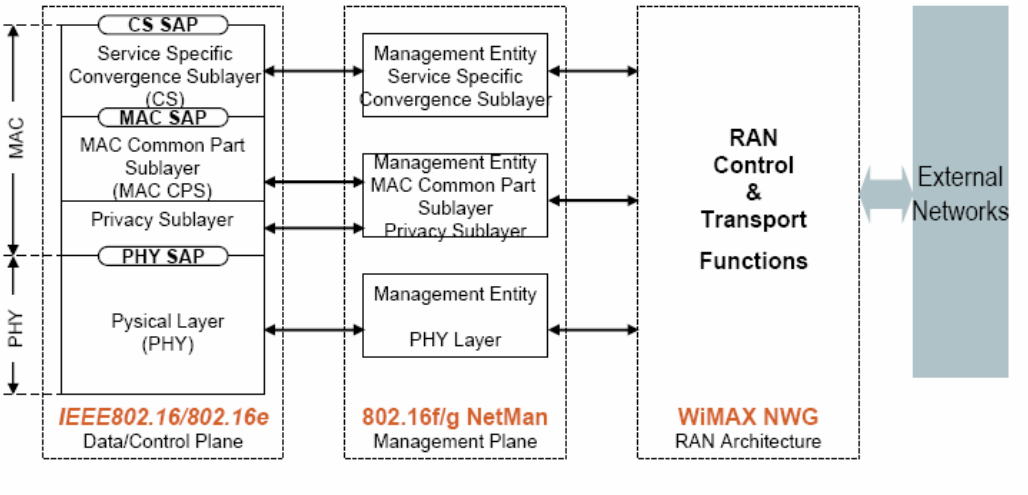

Fig. 1 802.16e Protocol Layer Architecture

This is usually achieved through the use of encryption. From the service provider's point of view, an important security consideration is preventing unauthorized use of the network services. This is usually done using strong authentication and access control methods. The service provider's need to prevent fraud should be balanced against the inconvenience that it may impose on the user. Security is an important consideration in any communications system design but is particularly so in wireless communication systems. In Networking, There are number of routing protocols for deciding the routes for efficient and reliable communication with no loss of packets and confidentiality of packet delivery. The protocols efficiency and security depends on different parameters such as end-to-end Delay, etc. WiMAX encrypts neither the MAC headers nor the MAC management messages, with the purpose to enable various operations of the MAC layer. Therefore, an attacker, as a passive listener of the WiMAX channel, can retrieve valuable information from unencrypted MAC management messages. Eavesdropping of management messages may reveal network topology to the eavesdropper, posing a critical threat to SSs as well as the WiMAX system.

3.2 Objectives of the Research Work

a) Implement the Wi-Max Network Security of MAC Layer using Cryptography.
b) To Implement the AES and RSA cryptography methods in Network Transmission.
c) To Analyze the Packet Delivery Ratio (PDR).
d) T obtains the Throughput of the different Network's scenarios.

4. PROPOSED METHODOLOGY

NS2 is used as simulation platform. According to the general network architecture of WiMAX all the communication takes place on the client server model where client acts as a mobile station and server as a base station. In this research paper we will design a wireless network in NS2 which comprises 2 hosts as Subscriber Stations (SS) and a server as a Base Station (BS) and will use AES, RSA cryptographic algorithm to secure the network and avoid the unauthorized access to the network.

1. Implementation of the network scenario of MAC Layer using different nodes/users.
2. Implementation of security algorithms on the network one by one such as AES and RSA.
3. For each Security Algorithm with variation in number of nodes, observing and noting the different values of each stated parameter for each protocol.
4. Generation of graphs for each parameter and comparison of results after combining results of respective graphs of each protocol.
5. Repetition of the above said steps of this flowchart with network scenario of multiple users and Stating of the results.

4.1Simulator Comparison

We will compare the performance of routing protocols with the help of ns-2 simulator and assumed multiple nodes to be used in the network scenario.
The following parameters are:

4.2 Throughput

Throughput refers to how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as Internet and network connections.

For example, a hard drive that has a maximum transfer rate of 100 Mbps has twice the throughput of a drive that can only transfer data at 50 Mbps. Similarly, a 54 Mbps wireless connection has roughly 5 times as much throughput as an 11 Mbps connection. However, the actual data transfer speed may be limited by other factors such as the Internet connection speed and other network traffic. Therefore, it is good to remember that the maximum throughput of a device or network may be significantly higher than the actual throughput achieved in everyday use.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

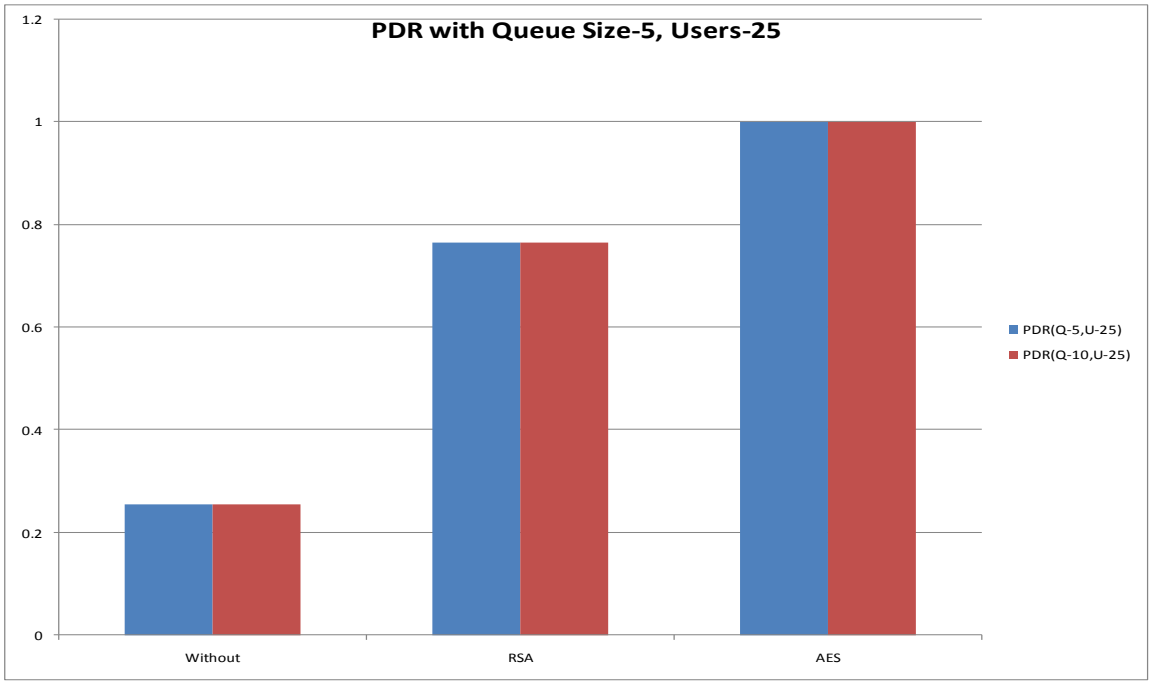

Figure 14: Packet Delivery Ratio Graph for AODV

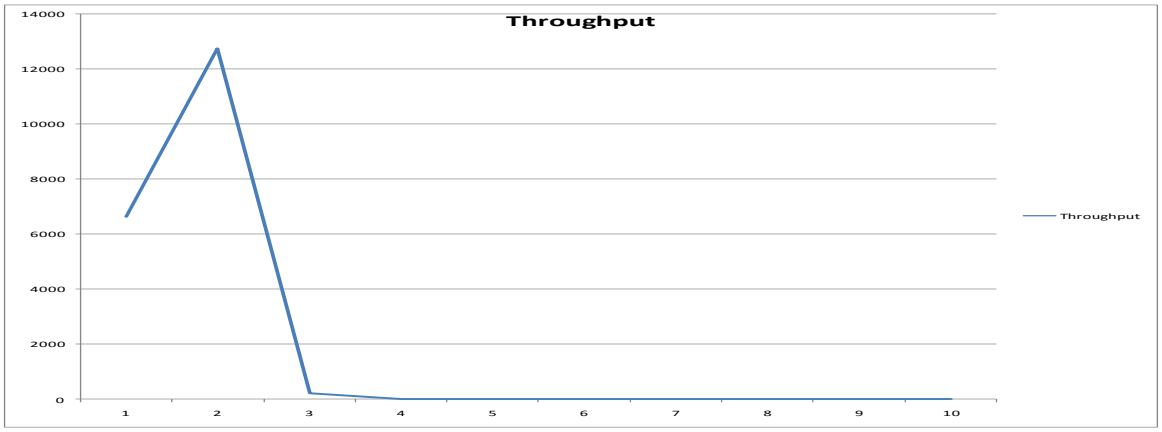

Figure 15: Throughput Graph for AODV

4.3 Packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.
Mathematically, it can be defined as:
PDR= S1÷ S2
Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

5 CONCLUSIONS AND FUTURE WORK

5.1 Nodes Description

In AODV routing protocol, there is need to be initialize the number of nodes to demonstrate that how the packets are transmitting from sender to receiver. We have taken the 25 nodes. Theses nodes are free to move in the networking environment and transmit the packets with path discovery.

5.2 Results of Routing Protocols

The results have been generated for the different protocols implementation and calculated the parameters such as throughput and PDR from sender to receiver with variation in queue Size and Number of Nodes.

The number of nodes has been created and calculated the desired values and drawn the graphs

Table designed according to the values used in Research work

Queue Size	Users/Nodes	PDR	Algo
5	25	0.255	Without
5	25	0.7649	RSA
5	25	1	AES
10	25	0.255	Without
10	25	0.7649	RSA
10	25	1	AES

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

6.1. CONCLUSION

In this project we have studied the performance analysis of the routing protocol with Cryptographic Methods such as AES and RSA on AODV using ns-2 simulator from the various authors described above in 802.11 networks. In this project, we calculate the packet delivery ratio, throughput for AODV MAC Layer.

6.2 FUTURE WORK

The above work will be conducted at the real time platform and it should also be tested on cross layer. The above work is conducted in MAC and Network Layer individually. But in future it can be tested on cross layer or combined layer i.e. MAC Layer + Network Layer. The work will also be conducted on the 802.15 and 802.16 standards. Further, the investigation can be done on security of AODV and improvement proposal for better secure communication in network environment.

REFERENCES

[1] Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski "IEEE 802.16 Security Issues: A Survey"16th telecommunication forum TELFOR 2008
[2] IEEE Std. 802.16e, air interface for fixed and mobile broadband wireless access systems. IEEE Standard for local and Metropolitan Area Networks, February 2006.
[3] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed "Fundamentals of WiMax" ", Feb, 2007
[4] J. Hasan, Security Issues of IEEE 802.16 (WiMAX), School of computer and Information Science, Edith Cowan University, Australia, 2006
[5] Syed Ahson, Muhammad Ilyas, "WiMax standards and security" CRC press, Sep 2007
[6] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed "Fundamentals of WiMax" "fig. 9.1", Chapter-9, PP 308, Feb, 2007
[7] D. Johnston and J. Walker, Overview of IEEE 802.16 Security, IEEE Security & Privacy, magazine May/June 2004.

DOI 10.17148/IJARCCE.2015.4904