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

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

Research and Analysis of WiMax Communication

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

Student, Department of Computer Science, JCD Vidhyapeeth, Sirsa, India[1, 2]

Abstract: WiMax means Worldwide Interoperability for Microwave Access. It is the wireless technology and enhancement of 802.16 standards. The forum describes WiMax as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". WiMax has many salient advantages such as: high data rates, quality of service, scalability, security, and mobility. In WiMax, security is the major issue for transmission of data from end to end. In this research paper we discuss about NS2 used as simulation platform, MAC layer and protocol Architecture of WiMax. 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.

Keywords: WiMax, Cryptography, AES, RSA, PDR.

I. 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 deception should 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.

II. PROTOCOL ARCHITECTURE

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). (Refer Fig.1)

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.

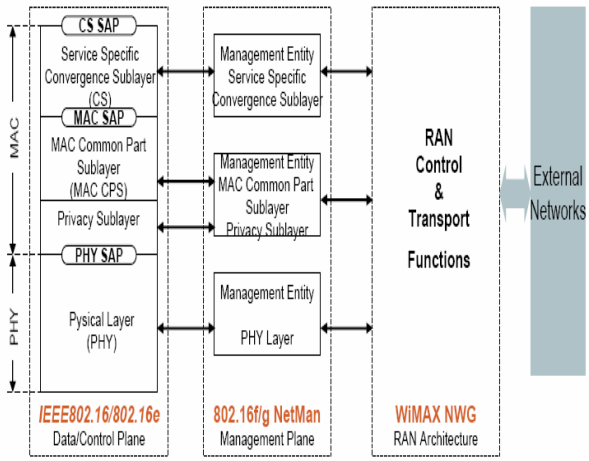

Fig1:802.16e Protocol Layer Architecture

DOI 10.17148/IJARCCE.2015.4970

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

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

It is also responsible for encryption and decryption of traffic passing from the PHY to the MAC layer and vice versa.

III. OBJECTIVES

A. 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. 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

B. Objectives of the Research Work

1. To implement the Wi-Max Network Security of MAC Layer using Cryptography.
2. To Implement the AES and RSA cryptography methods in Network Transmission.
3. To Analyse the Packet Delivery Ratio (PDR).
4. To obtain the Throughput of the different Network's scenarios.

IV. 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

A. Simulator Comparison

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

B. 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.

C. 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:

$$PDR = S1 \div S2$$

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.

V. FUTURE WORK

In this project we will calculate and compare the PDR and throughput results using three cases. i.e. without any encryption scheme, using RSA, using AES. We will discuss and study 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.

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.

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

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

VI. LITERATURE SURVEY

[1] Y. Hu, A. Perrig, and D. Johnson (2003), "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", INFOCOM.
The author has been assimilated the knowledge about possible attacks in networks and security issues in this regard. They introduced that in wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. They presented a new and general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and they present a specific protocol, called TIK, that implements leashes.

[2]Y. Ganjali and A. Keshavarzian (2004), "Load balancing in ad hoc networks: Single- path routing vs. multi-path routing", IEEE.
The author has been assimilated the knowledge about Load balancing in ad-hoc networks. They has been studied the Multi-path routing. It has been shown that using multiple paths to route messages between any source-destination pair of nodes (instead of using a single path) balances the load more evenly throughout the network. The common belief is that the same is true for ad hoc networks, i.e., multi-path routing balances the load significantly better than single-path routing. They introduced a new model for evaluating the load balance under multi-path routing, when the paths chosen are the first K shortest paths (for a pre-specified K). They explained that there should be very large number of paths for identifies the load distribution, but on contrary side, it is very costly and therefore infeasible. This is in contrary to the previous existing results which assume that multi-path routing distributes the load uniformly.

[3] JJ Garcia-Luna-Aceves, M. Mosko, and C.E. Perkins(2003), "A new approach to on-demand loop-free routing in ad hoc networks", ACM.
This paper describes the ROAM which is an on-demand routing algorithm that maintains multiple loop-free paths to destinations. They explained that each router maintains entries only for those destinations for which data flows through the router, which reduces storage space requirements and the amount of bandwidth needed to maintain correct routing tables. They explained ROAM that it routes are established and maintained on demand using diffusing computations. A router does not send updates for active destinations, unless its distance to them increases beyond a given threshold. ROAM maintains state that informs routers when a destination is unreachable and prevents routers from sending unnecessary search packets attempting to find paths to an unreachable destination. ROAM is shown to converge in a finite time after an arbitrary sequence of topological changes and is shown to be loop-free at every instant. The time and communication complexities of ROAM are analyzed.

[4] Osama H. Hussein, Tarek N. Saadawi (2005), "Probability Routing Algorithm for Mobile Ad Hoc Networks Resources Management", IEEE.
Author has been introduces a resource management application of a probabilistic-based ant routing algorithm for mobile ad hoc networks (ARAMA) that is inspired from the ant's life . Mobile ad hoc networks (MANETs) are highly dynamic, self-configured and self-built networks. The goal of this paper is to present ARAMA ability to manage MANET's resources by achieving fair network resources distribution, while considering the dynamic characteristics of MANETs and the need for low control overheads. This paper provides a description for the algorithm. In this algorithm, the nodes' (node's energy, processing power,) and links' (bandwidth,) parameters are measured and collected in the nodes' indices. A path index is used to measure the path total resources and serves to minimize the forward control packet (ant) size. The concepts of negative backward ant destination trail are introduced to enhance the performance of the algorithm. The simulation results show the potential of ARAMA to achieve fair energy usage across the network nodes as an example of the network resource management. More, the results show the general ability of the algorithm to solve MANET's routing problem.

[5] Mei-yu Feng, Sheng Cheng, Xu Zhang and Wei Ding (2007), "A Self Healing Routing Scheme Based on AODV in Adhoc Networks", IEEE.
The author has explained the routing schemes and many routing protocols have been proposed for ad hoc networks and many research works have been done to improve the performance of routing protocols. They explained that this cannot overcome the problems of edge effect and route break at same time without incurring heavy control overhead. In this paper, based on the analysis of routing problem, a self-healing routing scheme based on AODV (SHAODV) is proposed. In this scheme, routes can be constructed with long lifetime and unstable route can be self-heal to stable one before being broken absolutely. Simulation shows that the scheme wins lower average route overhead and lower times of route break than AODV.

[6] P. Pham, S. Perreau, and A. Jaya suriya (2005), "New Cross-Layer Design Approach to Ad Hoc Networks under Rayleigh Fading", IEEE.
The author has been assimilated the knowledge about design approach of Ad-hoc network and proposed a new cross-layer design employing the predictability of Rayleigh channels to improve the performance of ad hoc networks. They also explain a Markov model for Rayleigh

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

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

channels and an innovative Markov model for IEEE 802.11 distributed coordination function. By combining these two models, they derive the theoretical expressions for network throughput, packet processing rate, packet loss probability, and average packet delay under Rayleigh channels. The simulation of the proposed cross-layer design is also carried out. They shown that the new approach improves the network throughput, reduces unnecessary packet transmissions and therefore reduces packets lost. They also show that there is a close match between the analytical and the simulation results which confirms the validity of the analytical models.

[7] Satoshi Kurosawa (2007), "Detecting Black hole Attack on AODV-based Mobile Adhoc Networks by Dynamic Learning Method", International Journal of Network Security.
This paper analyzes the Black hole attack which is one of the possible attacks in ad hoc networks. In a Black hole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper, they propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of our scheme compared with conventional scheme.

[8] Vishnu K, and Amos J .Paul (2010), "Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications.
The author has explained the Black hole and gray hole attack in Mobile adhoc network. Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. In this paper they proposed complete protocol for detection & removal of networking Black/Gray Holes.

[9] K. Lakshmi, S. Manju Priya (2010), "Modified AODV Protocol against Black Hole Attacks in MANET", International Journal of Engineering and Technology.
The author has been explained the AODV routing protocol and modified the AODV file for Black hole attack implementation and analysis. In Mobile Adhoc Network (MANET), it consists of a collection of wireless mobile hosts without the required intervention of any existing infrastructure or centralized access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MANET is a complex issue. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security. They attempt to focus on analyzing and improving the security of one of the popular routing protocol for MANET viz. the Adhoc on Demand Distance Vector (AODV) routing protocol. The proposed solution is that capable of detecting and removing black hole nodes in the MANET at the initial stage itself without any delay.

[10] Vishnu K and Amos J Paul (2010), "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications.
Author explained that the inherent features such as-open medium, dynamically changing network topology, lack of centralized monitoring and management point, and lack of a clear line of defense of the MANET make it vulnerable to a wide range of attacks. There is no guarantee that a communication path is free from malicious or compromised nodes which deliberately wish to disrupt the network communication. So protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. They address the problem of packet forwarding misbehavior and proposed a mechanism to detect and remove the black and gray hole attacks. Author's technique is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets.

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.