Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.202 – 211

RESEARCH ARTICLE

SECURE DATA TRANSMISSION OVER WIMAX NETWORKS USING VPN TECHNOLOGY IN REALTIME ENVIRONMENTS

J.BALU*[1]
M.Tech Student
Department of Computer Science and Engineering
PRIST University Pondicherry, India.
jbalu27@gmail.com

DR.S.THIRUNIRAI SENTHIL*[2]
Head of the Department
Department of computer science and engineering
PRIST University Pondicherry, India.
razvi_zen@rediffmail.com

ABSTRACT

This paper reviews providing strong security is necessary for real time services of any wireless access networks. Wimax and LTE are the latest wireless broadband access networks support high data rate and mobility and become increasingly important as WiMAX data LANs are deployed for business, government and military applications. But free-space transmission introduces new opportunities for eavesdropping on Wireless data communications. What makes it worse is that the sender and the intended receiver have no means of knowing whether the transmission has been intercepted or not, so the eavesdropping is virtually undetectable. Several papers are dealt security stands out as a critical issue in the design and deployment of WiMAX networks but they are not dealt with real time in environment, But, this main contribution of this paper is to provide highly secure data transmission for real time services in real time environment while using Wimax networks, for that We introduces a Virtual Private Networks (VPNs) have emerged as an economic alternative to this current wireless network with building a private networks. VPNs provide security by integrating a set of authentication, encryption, and access control and session management components.

KEYWORDS - IEEE 802.16, WiMAX, security, VPN, MAC address Authentication, EAP, PKM, and PKMv2.

I. INTRODUCTION

WIMAX stands for Worldwide Interoperability for Microwave Access. It is the technology aimed to provide broadband wireless data access over long distances. It is based on IEEE 802.16 standards and the standard defines only the physical (PHY) layer and MAC layer functionalities. The technology provides basic Internet Protocol (IP) connectivity and connection oriented wireless communications to the end users. The initial IEEE 802.16d standard is specific to fixed and nomadic users. Based on increasing mobile user requirements and to increase the coverage region, the IEEE standard released the 802.16e and 802.16j versions. Currently, the IEEE 802.16m task group is working to support the IMT Advanced requirements. The existing security issues in mobile WiMAX networks and QoS improvements are considered in IEEE 802.16m standard and it has full backward compatibility and interoperability with the legacy systems. The PHY layer functions are specific to physical transmit receive functions and wireless channel types. The MAC layer functions are divided into three sub layers: MAC convergence sub layer for data plane functions such as packet processing and etc.; MAC common part sub layer for MAC control functions; and security sub layer to provide the strong security for both network and users. The MAC security sub layer specifies the security functionalities and its implementations. The security sub layer supports are to: (i) authenticate the user when the user enters into the network, (ii) authorize the user, if the user has provisioned by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic. An overview of security functions defined in the standards is discussed in section II. Even though the IEEE 802.16 standards provide well defined security architecture, some security issues still exist due to unauthenticated / unencrypted MAC control messages. Many existing research efforts suggest solutions for each security threats based on public key management (PKM) protocol and some of ISPs have tried IPSec in practice for the implementation perspective. The default security mechanism provided by the layer-3 virtual private networks (VPNs) is IPSec. While providing strong security for an access network with IPSec, the existing QoS support should not be affected. Similar studies have been conducted only in simulations. Actual experiments and measurements are essential for practitioners and researchers for better analysis. In this paper, the QoS parameters such as subscriber station (SS) connectivity, one ASN with SS of other ASN are evaluated with test bed experiments for both standard IEEE 802.16d WiMAX MAC layer security and IPSec on top of MAC security.

The figure 1 shows the basic architecture of Wimax networks are subscriber station (SS), ASN makes connectivity to BS called Access service providers(AP) and CSN is a Network service provider used to make a connectivity to the application service provider(ASP) such as IP and internet.

Based on the test results, the security level, scalability and QoS support of each scheme is analyzed. In Section II describes the over view of Wimax security issues such as threat to MAC layer and Network layer. In Section III describes the security issues of Wimax network and solution of the existing method, draw back and proposed method with solutions. In Section IV describes implementation of proposed three tier security system of level of each scheme is analyzed. In Section V describes implementation Results and Discussions of proposed network architecture formation and data transmission are taken place in simulation tool and the last section V is the conclusion and future work.

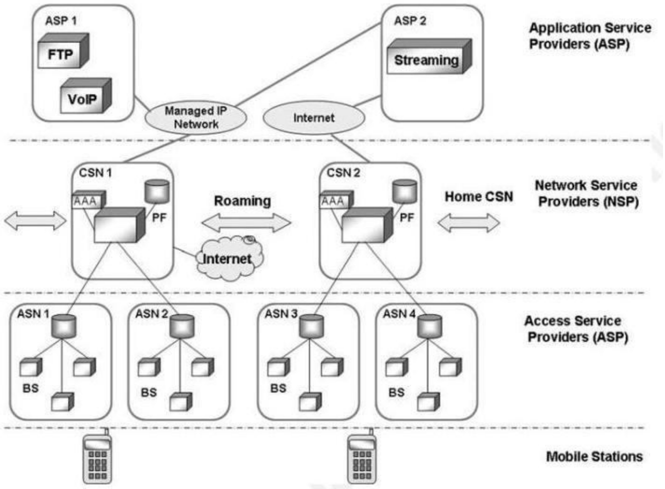


Figure 1. WiMAX network architecture

II. OVER VIEW OF WIMAX SECURITY ISSUES

WIMAX has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack including interception, fabrication, modification, and replay attacks. In this section some possible threats or vulnerabilities will be reviewed.

A. Possible Real time Threats

1. Could not identify the user if who sent malicious/threatening mail.
2. Causes Revenue leakage by the users to the service providers if they have an agreement for revenue sharing per user basis.
3. Couldn’t make log details of the users if MAC address is not bound with username.
4. Couldn’t use for WI-FI networks, since its is 2.4 GHZ licensed free spectrum.
5. Easy to hack data by unauthorized users if MAC level security is not done.

B. Threat to the MAC Layer

The MAC layer is connection oriented. There are two kinds of connections: management connections and data transport connections. Management connections are of three types: basic, primary, and secondary. A basic connection is created for each MS when it joins the network and is used for short and urgent management messages. The primary connection is also created for each MS at the network entry time, but is used for delay-tolerant management messages. The third management connection, the secondary one, is used for IP encapsulated management messages (e.g., dynamic host configuration protocol [DHCP], simple network management protocol [SNMP], trivial file transfer protocol [TFP]). Transport connections can be provisioned or can be established on demand. They are used for user traffic flows. Unicast or multicast can be used for transmission.

C. Threat to the Network Layer

1. DoS/Reply attacks during an MS initial network entry.
2. Latency and re-authentication issues during handovers.
3. Downgrade attack and bandwidth spoofing.

4. Cryptographic algorithm computational efficiency.
5. Hop-by-hop authentication issue in a multi-hop network.
6. Tunnel mode data forwarding issue in a multi-hop network.
7. Network coding issue in a IEEE 802.16m network.

III. SECURITY ISSUES AND SOLUTIONS

A. Existing Method

The previous research problems are mainly prevailed in the section of security is authentication based on only with username and password. The information may be hacked by unauthorized users while data travels in an public path (i.e.) internet, if user name and password are easy to traceable

Drawback

These methods are provide for the users to get authentication to access data and not for the securing their data.

B. Proposed Work

To review and design a new methodology to provide secure data communication for the users to access wireless broad band when using of WiMAX .In this paper using VPN technology designed to provide a Three Tier Security mechanism for data communication with PKM (public Key Management) method to make highly securable data communication are

Level 1

(i) First verify the MAC address of the Wimax devices of the user with their location.

Level 2

(ii) Second match this MAC ID with the user name and password of each user.

Level 3

(iii) Third the VPN server/Router allot an IP address to the corresponding user only if ASN verifies both MAC address and the user name and then provide VPN tunnel using PPTP protocol. This provides a virtual path like a private path between the users while communicating evens they are located in different places.

The figure 2 shows the proposed network architecture diagram for how to make a secure communication by using VPN on Wimax Networks in real time environment. It consists of User A and B with Wimax devices, switches, ASN and CSN servers and VPN Router. User A and B of PC s are connected to Wimax devices with Ethernet cables other than wireless interfaces.

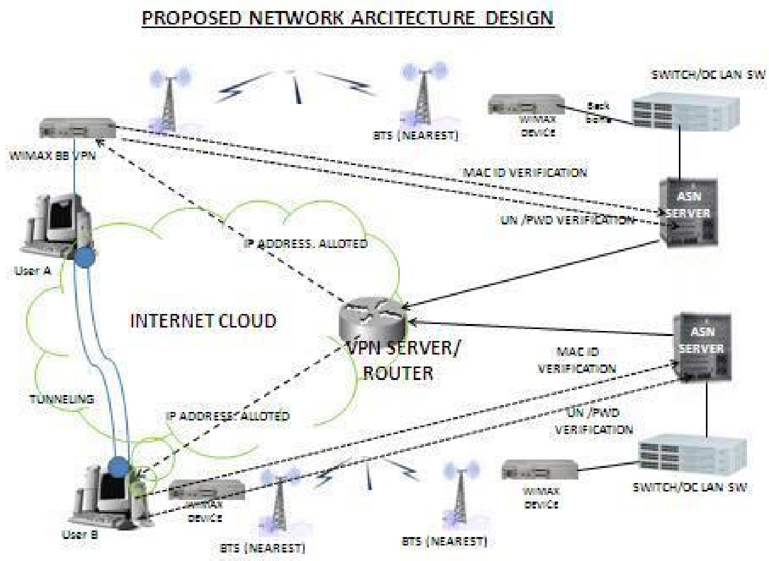


Figure 2. WiMAX over VPN network architecture

Algorithm

1) User A make a request to access user B of same concern located in different places.

2) ASN server verifies the MAC address of the Wimax device of user A with their location. if MAC address matches then ASN allow

3) User A to go for enters username and password, ASN server verifies the both MAC address and username and password. If matches correctly send to VPN Router or Server.

4) VPN Router verifies the user name and password of user A, if matches, it allot the IP address to user A.

5) The same procedure repeated for the user B side ,

6) MAC address of the Wimax device of user B and username and password of the user B verified by the ASN server if both are matched ok, then

7) VPN Router/server allots the IP address to the user B.

8) VPN server creates a tunneling between user A and user B.

9) Now the users can make communication by using dedicated path between them. No hackers can't intrude in this tunnel path and hack the information of either user A or user B.

10) Virtual path will be removed if any one of the user Disconnect the services

IV. IMPLEMENATION

A. Modules

- MAC Address verification
- Key management
- IP address allotted by VPN server act as CSN server.
- Implementation by NS2 simulation tool.

B. Implementation Flow Chart

The figure 3 shows the steps of this algorithm for implementing the proposed secure data transmission on wimax architecture by using VPN.

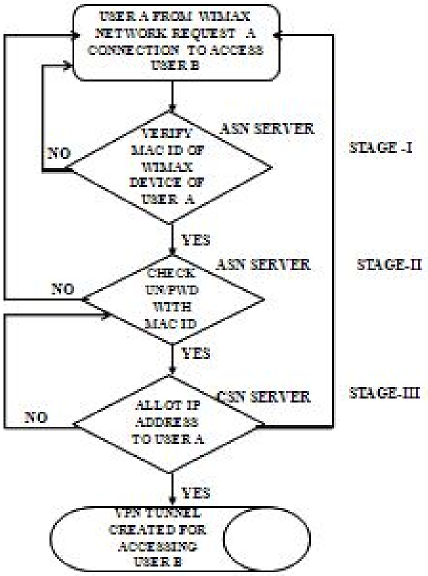

USER A FROM WIMAX NETWORK REQUEST A CONNECTION TO ACCESS USER B
VERIFY MAC ID OF WIMAX DEVICE OF USER A
ASN SERVER
STAGE -I
NO
YES
CHECK UN/PWD WITH MAC ID
ASN SERVER
STAGE-II
NO
YES
ALLOT IP ADDRESS TO USER A
CSN SERVER
STAGE-III
NO
YES
VPN TUNNEL CREATED FOR ACCESSING USER B

Figure 3. Implementation Flow Chart

MAC-ID Verification

MAC	ASN –USER NAME
4a6186b2c1fc	user_a
206a860b375f	user_b
fec154de7797	user_c

Figure 4. MAC address Management

Figure 4.2 shows the management of MAC addresses of the Wimax devices corresponding to the user are stored in ASN server. ASN is a database server like oracle/mysql or MS-Access depends on the service provider.

Key Management

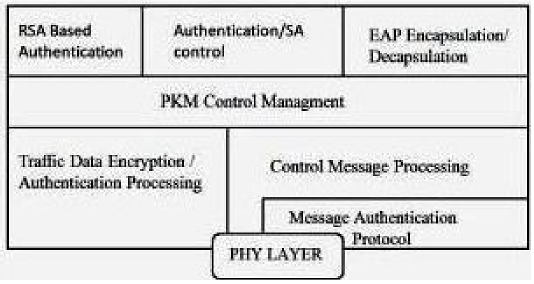

RSA Based Authentication
Authentication/SA control
EAP Encapsulation/ Decapsulation
PKM Control Managment
Traffic Data Encryption / Authentication Processing
Control Message Processing
Message Authentication Protocol
PHY LAYER

Figure 5. WiMAX Security Architecture

Figure 5 shows Wimax security architecture with EAP method of Key management. The model PKM key generation is given below as secure log file.

```
Jyang Pluto [5341: I Key ID: a0 ba 99 ed 00 f7 d9 f4 a6 f3 48 f3 fc c4 23 22
Jyang Pluto [5341: I Peer's ID is ID-KEY-ID: 'aOba99edOOf7d9f4a6f348f3fcc42322'
```

IP Address Management

IPSec.conf file of user A	IPSec.conf file of User B
Interfaces="ipsec0=eth1"	interfaces="ipsec0=eth0"
ip-assigned=192.168.2.105	ip-assigned =192.168.1.225
subnet= 192.168.2.0/24	subnet= 192.168.1.0/24

Figure 6. WiMAX Security Architecture

V. RESULTS AND DISCUSSION

A. Wimax Network Architecture formation

Simulation results are obtained by NS2 Tool. The Figure 7.shows the NAM output of proposed VPN over Wimax network architecture. It consists of 3 ASN servers, 1 CSN server provides communication to the Wimax devices via ASN and 9 APs (Access Point). The Wimax nodes are connected to ASN via APs.

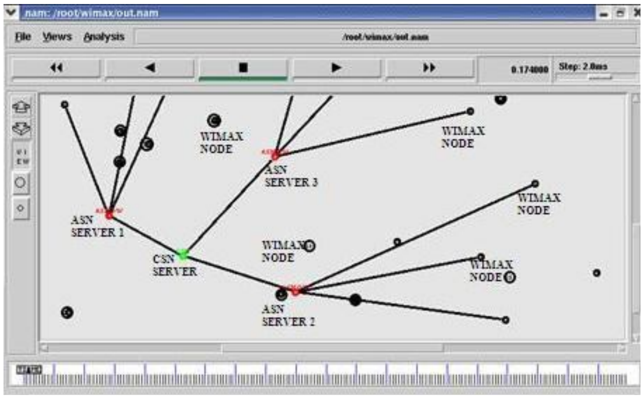
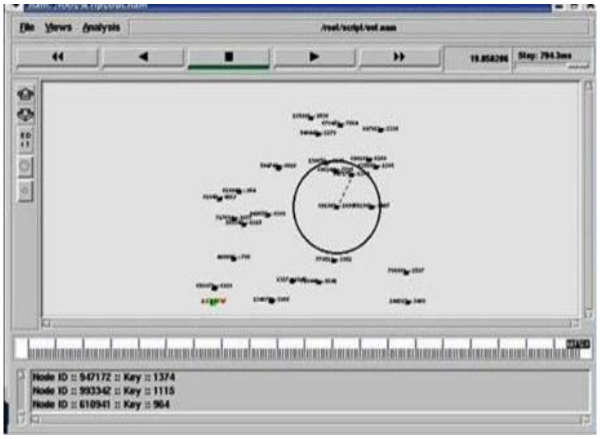


Figure 7. NAM output shows WiMAX architecture design

Data Transmission

The figure 8 shows the model simulation result of VPN connectivity between two nodes like a point to point connection even both nodes are connected to two different located ASN1 and ASN2 servers.



```
Node ID :: 947172 :: Key :: 1374
Node ID :: 993342 :: Key :: 1115
Node ID :: 610941 :: Key :: 964
```

Figure 8. Data transmission using VPN path

B. Performance Analysis

Throughput

In the simulation analysis for the Wimax networks, we found that the throughput efficiency during the speed of 3.5 Mbps the packet size in bytes is gradually increased from zero value to the maximum of 1000 data bytes. The figure 9 shows the gradual increase in the throughput reaches maximum is found to be at the steady state level. The analysis shows that the stable efficient condition for the MAN network area establishment using wireless Broadband access has better performance under the simulation environment.

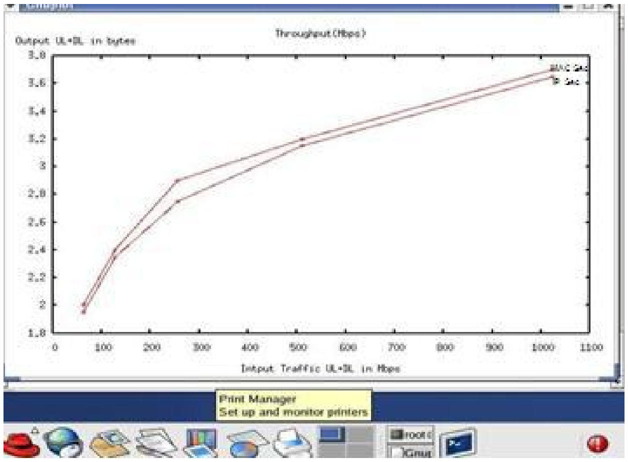


Figure 9. Packet size vs. Throughput

Packet delay:

In the simulation analysis for the Wimax networks. We found that the Packet delay during the simulation time of zero seconds is gradually decreased from 98 % to the minimum of 96%.

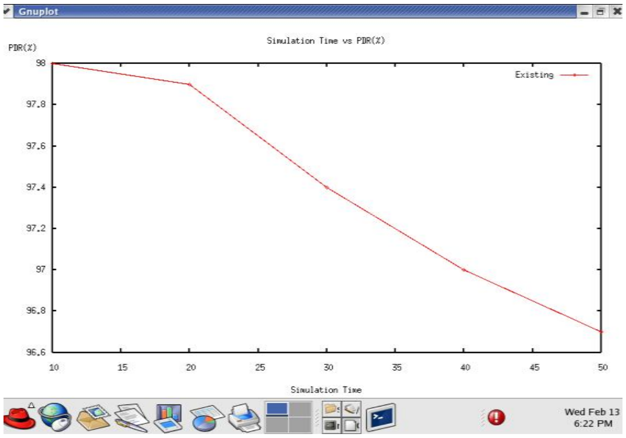


Figure 10. Packet drop vs. Simulation Time

The analysis shows that the minimum packet delay condition is achieved in the MAN network area establishment using wireless Broadband access has better performance under the simulation environment. Figure 10 shows the packet drop has been reduced from 10 seconds to 50 seconds**.**

C. Analysis of this Wimax Security schemes

Three security schemes are considered for this analysis, (i) WiMAX MAC layer security defined by the standards and (ii) EAP based Key security schemes (iii) for IPSec security on top of MAC layer security from practical implementations and from theoretical studies are analyzed for IPSec security on top of MAC layer security. WiMAX networks have well defined QoS architecture and security mechanisms defined by the IEEE 802.16 standards. But it has some security issues due to achieve the QoS unencrypted/unauthenticated MAC messages. From the practical perspective, ISPs have tried IPSec tunnels with MPLS VPN for fixed Wimax and mobile Wimax networks, because MPLS is very good security system providing class of services and provide high secure data transmission over wired and wireless networks without affecting the QoS especially for the users using Wimax networks for their data transmission.

VI. CONCLUSION

In this paper, the secure data transmission over WiMAX network using VPN technology are evaluated for both MAC layer security and IPSec using test bed experiments. Even though IPSec provides strong data security using IPSec tunnels for both wired and wireless networks, The QoS performance can be improved by using MPLS technology along VPN. However, no articles have reported actual experiments on or real measurements of the overhead of IPSec. This paper presents results from test bed experiments which are both practically and theoretically important for further analysis and comparison. Based on the existing research, modified IPSec may be combined with mobile IP (MIP) to support the mobile WiMAX networks.

REFERENCES

[1] H. Bourdoucen, A. Al Naamany and A. Al Kalbani. "Impact of Implementing VPN to Secure Wireless LAN" International Journal of Computer and Information Engineering 3:1 2009.

[2] Deepak Kumar Mehto, Rajesh Srivastava," An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile Wimax", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4,September 2011.

[3] Park, Shihyon Matthews, Bradley; D'Amours, Danny, McIver Jr., WilliamJ "Characterizing the Impacts of VPN Security Models on Streaming Video",Page(s) 152–159,Communication Networks and Services Research Conference Eighth Annual,11-14May 2010.

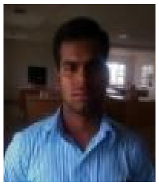
[4] Levon Nazaryan, Emmanouil A. Panaousis, and Christos Politis "IPSec Provisioning in WiMAX Networks for end to end communication.," IEEE VEHICULAR TECHNOLOGY MAGAZINE, Vol-10,pages 1556-6072 MARCH 2010.

[5] Dhaini, A.R. Dept. of Electr. & Comput. Eng.,Univ. of Waterloo, Waterloo, ON, Canada Pin-Han Ho ; "Performance Analysis of QoS Layer-2 VPNs over Fiber-Wireless (FiWi) Networks ," pp. 1-6 IEEE Global Telecommunications Conference October2010".

[6] Dhaini, A.R. ON, Canada Pin-Han Ho; Xiaohong Jiang ,"WiMAX-VPON: A Framework of Layer-2 VPNs for Next-Generation Access Networks "Optical Communications and Networking, IEEE/OSA July 2010," Journal of Vol: 2,Pages: 400 – 411

[7] Kejie Lu, University of Puerto Rico Yi Qian, NationalInstitute of Standards and Technology Hsiao-Hwa Chen,National Cheng Kung University Shengli Fu, University of North Texas "WiMAX Networks from Access to Service Platform ," IEEE Network, May/June 2008, vol. 8, pp. 0890-8044, June. 2008.

AUTHORS PROFILE



Mr.J.BALU, Presently Pursuing Final Year M.TECH CSE, In PRIST University, Puducherry Campus, Puducherry, India

Dr.S.THIRUNIRAI SENTHIL,M.C.A,M.Phil.,Ph.D., Sri Vinayaka Mission University Salem, in 2010, Presently he is a Working Professor, Head Of Department in Computer Science and Engineering at PRIST University, Puducherry Campus, and Puducherry, India. The area of specialization is an Data Mining, Computational Biology and Bioinformatics about the professional analysis