Investigation of Internet Key Exchange (IKE) In terms of Traffic Security with Gateway Security (GSE) In WiMAX Network

Rakesh Kumar Jha
Department of Electronics and Communication Engineering,
SVNIT, Surat, INDIA

Wankhede Vishal A
Department of Electronics and Communication Engineering,
SVNIT, Surat, INDIA

Upena D Dalal
Department of Electronics and Communication Engineering,
SVNIT, Surat, INDIA

ABSTRACT
In this paper, we identify and study a novel approach to secure WiMAX network for IKE (Investigation of internet key exchange) in terms of traffic security with the help of gateway security (GSE).Propose work has been applied on Location based network and we have observed the performance analysis of this attack on both type of network possible in WiMAX i.e Packet CS and ATM CS networks. We have done investigation on ASN-GW security with AES, 3 DES and MD5.IPSec is the primary Protocol use in wireless for traffic protection between the communicating entities. It operates on Network Layer and provides protection IP Datagram by encapsulating it into ESP tunnel. In security architecture there are security sublayer for data exchange between the MAC layer and PHY layer. There is no any security Layer has been provided between (ASN and BS) Network Layer/ IP Layer to application layer so this area is still a good for Research for security issues in WiMAX. We have proposed on Gateway security (GSE). In last phase we have given performance comparison between all four conditions with four scenarios. Analysis based on network simulation tool OPNET Modeler 14.5.

General Terms
Security issues in WiMAX network.

Keywords
WiMAX, Security Analysis, IKE, GSE, Packet CS, ATM CS, AES, MD5, RSA Signature, OPNET Modeler

1. INTRODUCTION
Network security is concerned with the secure transmission of traffic between the network elements. These network elements can be from the same network domain or from different domains, where the network domain is referred to a network administered and maintained by a single operator. The security parameters and security policies within a domain are usually identical because they are implemented by the same operator. IPSec is the major security parameter that is applied on WiMAX network domain security to secure data traffic between different networks and also within the same network by providing data integrity, source authentication and anti-reply protection. It operates on Network layer and provides security between two GSEs or GSE and Network Elements. IPSec facilitates the network in terms of selection of appropriate protocols and algorithms to be applied on the links supposed to be guarded. The major elements of IPSec are security protocols is uses, security association it create and maintain with the help of these protocols, secret keys management used for authentication and encryption procedures and the encryption algorithm to encrypt the data traffic between communicating nodes.

2. NDS/IP INTERFACES
The interface between two different network domains is denoted by Ra in NDS/IP (**Figure 1**). The Ra interface is used to implement security parameters between two different security domains to protect transportation of data between the domains in question. As security parameters data Authentication and Data Integrity protection is mandatory to be implemented while data encryption is not compulsory but strongly recommended to implement to avoid any kind eavesdropping and date loss or alteration. On the other hand RB is the interface that provide secure link between the elements within a security domain. Like Ra It is mandatory to implement data authentication and data integrity parameters and data encryption is optional. Data integrity, data authentication and data encryption are the main policies implemented on network domain interfaces and provided with the help of ESP, Security Gateway GSE and IKE (Internet Key Exchange). Internet Key Exchange is used by GSE to create and maintain an ESP tunnel for the sake of secure transmission of data traffic across the GSEs or in other words across the networks. Since the Ra interface provide the protection services inside a network domain, it is obvious that the security policies implemented on RB is totally on the will of network operator. The operator decides the security services like firewalls etc to be implanted in the network domain.

3. GATEWAY SECURITY
Implementation GSEs are the gateway to the inbound and outbound data traffic to and from a network and implemented at the border of the IP security domain to provide traffic security. Since GSEs uses Ra interface then it is obvious that it imposes Integrity, Authentication and Data Encryption in the network domain. All the NDS/IP traffic (incoming and outgoing data) has to go through security gateway. A network domain security can have more than one, depending on the situation. For example if the size of the network is too large to be handled by a single gateway or the data traffic is very often and a single GSE cannot handle it (load harmonizing). Also to avoid a single point failure or for redundancy issues more than one GSEs can be introduced in a single network. GSEs implement the security policies designed for the gateway and enforce it on the networks generating the data traffic transmission. Since GSEs are security implementation entities, it should be physically secured from malicious access. Each GSE is supposed to be paired with the communicating network GSE with at least of an IPSec tunnel

to transport the traffic. Also it is the job of GSE to establish Security Associations SAs with the counterpart on the other end. The SAs are established with the help of a key exchange procedure involving Internet Key Exchange IKE protocol. It is the important factor to know that SA is one way traffic association and therefore every GSE should have at least a pair of SAs one each for incoming and outgoing traffic For the sake of authentication GSE use Internet Security Association and Key Management Protocol (ISAKM).

4. SECURITY ASSOCIATIONS DATABASE (SAD)

It is a database of all the security associations created between GSEs or Hosts and GSEs. Actually the data traffic is tunneled according to the security polices in SPD to SAs, and there is criteria or mechanism for deciding that to which SAs and how the traffic should be forward. This information should be shared between the communicating entities and both the communicating parties must be agreed upon. GSEs use an indexing technique to access and identify the SAs that have to be involved in prospected transmission. This indexing in GSEs is called Security Parameter Indexing (SPI).

The Authentication used in this WiMAX is two types' network authentication algorithms and encryption algorithms. MD5 and SHA-Paper are used to provide authentication and integrity while triple DES-CBC and AES-CBC are the algorithms responsible for data encryption or data confidentiality. Although there is DES algorithm that can be used for encryption but the network security design engineers recommend the use 3DES instead of DES because of the weak key structure of DES.

5. SECURITY PROTOCOL

IPSec security is network layer protection and implemented on Ra and RB interfaces to provide protection to the data traffic between two communicating entities in Proposed Networks. IPSec need to be implemented with the help of two protocols Authentication Header AH and Encapsulated Security Payload (ESP). These protocols can be implemented separately or in a combination/nested manner in two different modes; transport mode and tunneled mode. Both of these modes have different approaches towards security behavior, in transport mode the foresaid protocols secure the upper layer protocols and only IP header of the IP datagram packet is secured while in case of tunnel mode, the data traffic between the communicating network nodes is tunneled to provide protection against security threats and the full IP datagram is protected including IP header. A host should support both the transport mode and tunneled mode but in GSE must only support tunnel mode. In case if a GSE is supporting both the tunneled and transport layer then it must be a security gateway that also acts as a host e.g. a GSE that is equipped with network management functionality. IPSec use Encapsulated Security Payload (ESP) protocol for data integrity, source authentication and data encryption. As mentioned earlier that ESP have two modes; transport mode and tunnel mode and IPSec use the tunnel mode of ESP to secure the whole IP datagram packet instead of only protecting IP header. The security parameters used are stored in security policy database and depend on the security associations. These parameters define the set of services that are provided for protection and are they are agreed upon at the time of security association establishment. If authentication of data source is selected to be a part of the security association then anti-reply service has to be selected and its selection is only dependent on the receiver

6. SECURITY ASSOCIATIONS

Security Association is a virtual relationship between two GSEs consisting of a set of agreements about security parameters to be used to protect the traffic flow. The agreement detailed information must be agreed upon by both the communicating entities and shall be shared between them. In IPSec security associations are the most important aspect and both AH and ESP protocols use SAs as vehicle for transportation and implementation of security policies. It identifies how the security services are to be implemented. Security associations supposed to support different encryption algorithms, authentication procedures, secrete key negotiation and maintenance and other security parameters to assist IPSec and other protocols used in communication. Protocols use the security association to identify how the security services have to be implemented. Security Associations must also support host-oriented certificates for lower layer protocols and user-oriented certificates for higher level protocols. A security association is unidirectional virtual link and can only be used for unidirectional traffic, this is the reason that every GSE has to maintain at least two SAs with its counterpart to provide support for bidirectional traffic i.e. one SA each for incoming traffic to the network and outgoing traffic from the network. The security parameter index (SPI) from security association database and destination IP address is used to specify the concerned SA for each IP packet to be transmitted

6.1 Encryption Algorithms

Encryption is actually data encoding with the help of a secrete key to make it un-understandable for unauthorized recipient. The encoded data is called cipher text and is decoded on the receiver end with the help of the encryption/decryption key. The decrypted data is also referred to plain text. Encryption algorithms as mentioned earlier are responsible for data confidentiality. The IP datagram traffic between two networks entities (between the entities of the same or different network) need to be encrypted to avoid any kind of security threat to the traffic flow.

6.2 Advanced Encryption Standards AES

AES is the encryption algorithm standard which was selected by National Institute of Standards and Technology NIST in an open competition prevailed for four years. It has been selected from five finalists on the bases of security, free availability; 128 bits block size, support of different key sizes 128 (IEEE 802.16 Std.), 192 and 256 bit, flexibility and computational efficiency. AES is supposed to be the successor or replacement of Data Encryption Standards after it would be obsolete and IETF recommends it to be the IEEE 802.16 STDs. Encryption algorithm for IPSec ESP protocol for data confidentiality. The AES used by ESP protocol in WIMAX is fixed to operate on Paper28 bit key which is the IEEE 802.16 STDs. Key length of AES; it is also referred to Rijndael algorithm.

7. NETWORK MODEL

This section describes the implementation of WiMAX network using OPNET Modeler 14.5 and the Performance Analysis of the network model on the basis of IKE (Investigation of internet key exchange) in terms of traffic security with the help of gateway security (GSE). The network model design contains two network scenarios; the first scenario based Packet CS with AES Security on Router and BS and the second scenario based on the ATM CS with

AES Security on Router and BS. This network model is shown in **Error! Reference source not found.**The whole WiMAX network is implemented on the map of INDIA as shown.

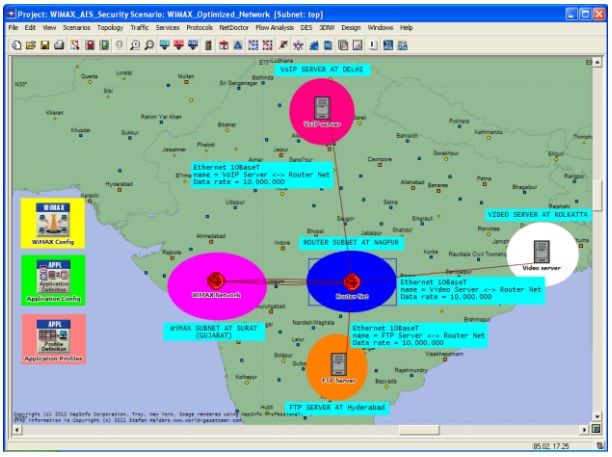

Fig 2: Packet CS Network

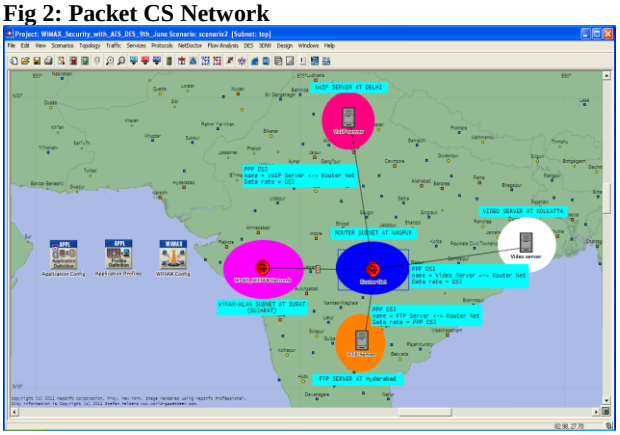

Fig 3: ATM CS Network

As shown in above **Figure 2 and Figure 3**, the network model contains three (3) application servers to provide service to the clients. These servers are; VoIP server with an application of IP Telephony (PCM Quality) is placed at Delhi (INDIA), the Video Server with an application of Video Conferencing (Light) is placed at Kolkata (INDIA) and an FTP Server with an application of File Transfer (Light) is placed at Hyderabad (INDIA). Also two (2) subnets are present in the network, these subnets are; Router Subnet and WiMAX Subnet. The router subnet provides route to the packets coming from servers to reach the clients. The WiMAX subnet provides the complete distribution of WiMAX clients in a cell based structure. The Router subnet is placed at Nagpur (INDIA) which is shown in Fig This subnet contains the ASN – GW (Access Service Network – Gateway) and the Ethernet routers. The ASN – GW provides the connection between the Application Servers and the WiMAX network. The servers which are used in the network are Ethernet Servers using Ethernet links. The packets generated from the servers are first passes through ASN – GW and then it gets route to reach the WiMAX network. The link used to connect Servers and ASN – GW is Ethernet 10BaseT link. From the ASN – GW the packets transmitted to the routers; Router A, Router B, and Router C through Ethernet 100BaseT link in order to improve performance of the whole network.

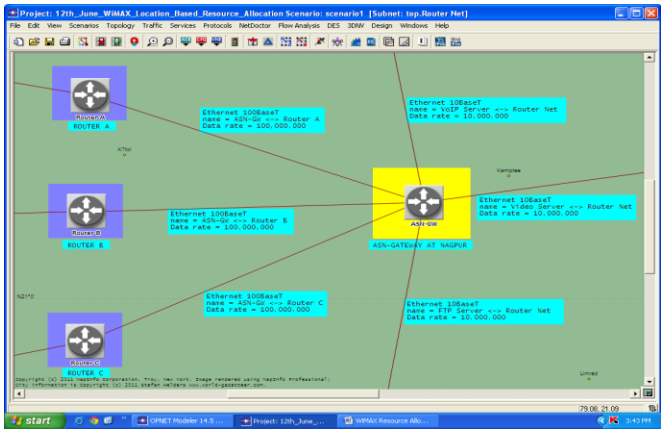

Fig 4: Router Subnet of WiMAX Network

Another subnet is WiMAX subnet which is shown in Figure 4

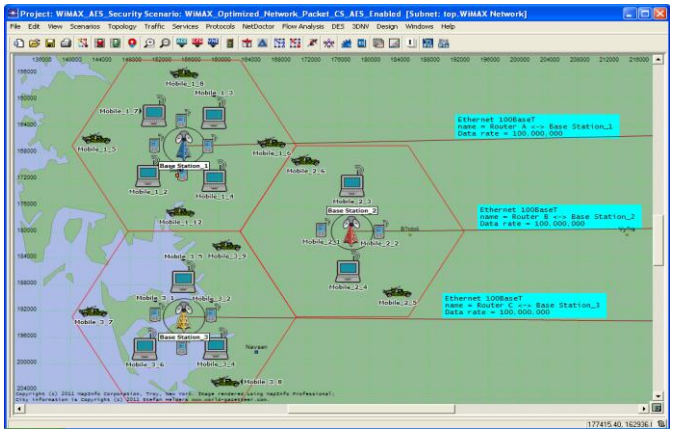

Fig 5: Packet CS network with AES Security

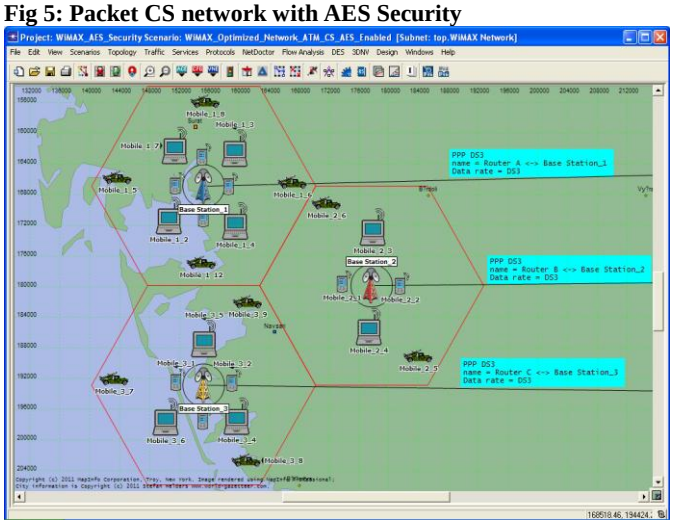

Fig 6: ATM CS network with AES Security

Figure 6. WiMAX Subnet of WiMAX Network This subnet is placed at Surat District (Gujarat - INDIA); in this subnet there are three (3) WiMAX cells. According to IEEE 802.16 standards the cell radius of one Base Station (BS) is 50 kms theoretically and 30 kms practically, in our case we kept the cell radius to 15 kms so that the distance from one BS to another BS is 30 kms. Cell 1 with Base Station 1 (BS1) is placed near Surat (Gujarat - INDIA); this cell is shown in **Fig 7.**

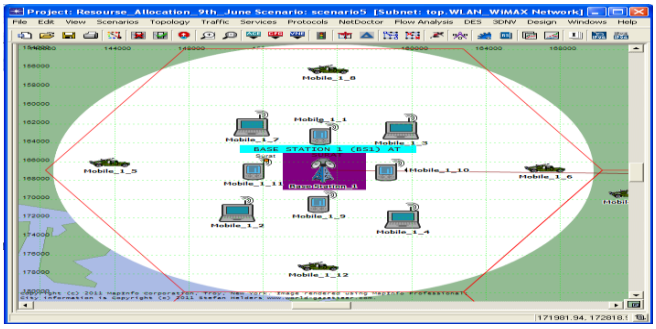

Fig 7: Cell 1 with BS1 in WiMAX Subnet

In this cell there are 12 WiMAX Subscriber Stations (SS), these SS are distributed randomly throughout the cell. The Subscriber Stations (SS) which are closer to Base Station (BS) is called Aggressive node and the modulation scheme is set to 64 QAM with ¾ coding rate. The Subscriber Stations (SS) which are far from the Base Station (BS) is called Conservative node and the modulation scheme is set to 16 QAM with ½ coding rate. The Subscriber Stations (SS) which are very far from Base Station (BS) i.e. near the edges of the cell has the modulation scheme of QPSK with ½ coding rate.

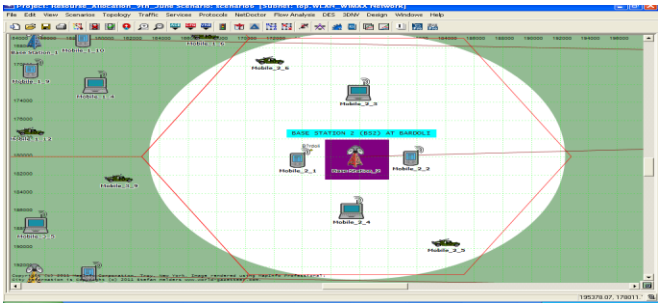

Fig 8: Cell 2 with BS2 in WiMAX Subnet

Cell 2 with Base Station 2 (BS2) is placed near Bardoli (GUJ.); this cell is shown in **Fig 8.** In this cell there are 6 WiMAX clients, these clients are distributed randomly throughout the cell having the same modulation schemes as discussed above. Cell 3 with Base Station 3 (BS3) is placed near Navsari (GUJ.); this cell is shown in **Fig 9**. In this cell there are 9 WiMAX clients which are distributed randomly throughout the cell with same modulation as discussed above.

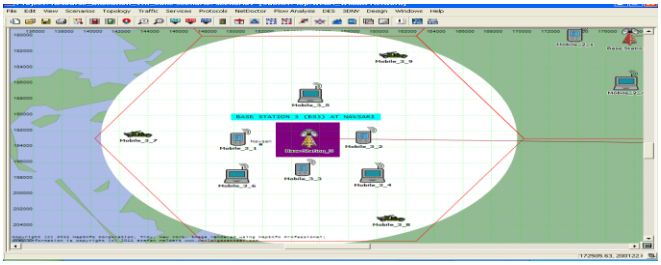

Fig 9: Cell 3 with BS3 in WiMAX Subnet

Base Station 1 (BS1) is in contact with router an in router Subnet through 100BaseT Ethernet link; similarly Base Station 2 (BS2) and Base Station 3 (BS3) are in contact with Router B and Router C in Router Subnet respectively. In second Scenario the WiMAX Network Model is completely same, but only the difference is, there is one Misbehaving Node in each cell in WiMAX Subnet. This Subnet with Misbehaving Node is shown in **Fig**

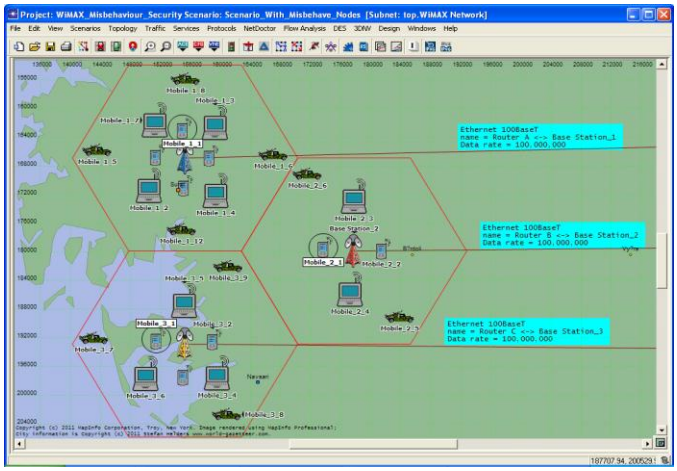

Fig 10: WiMAX Subnet with Misbehaving Node

The Misbehaving Nodes in each cell are highlighted in the figure. These Nodes are Mobile_1_1 node in Cell 1, Mobile_2_1 node in Cell 2 and Mobile_3_1 node in Cell 3.

8. SIMULATION PARAMETERS

All the parameter involved in this Network models is given in **Figure 11, Figure 12 and Figure 13.**

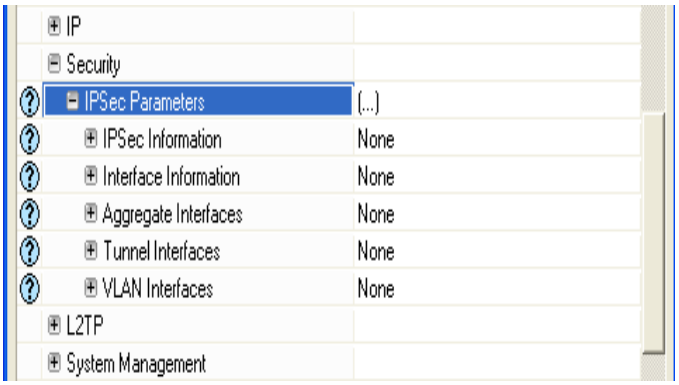

Fig 11: IP Sec Parameters without Security

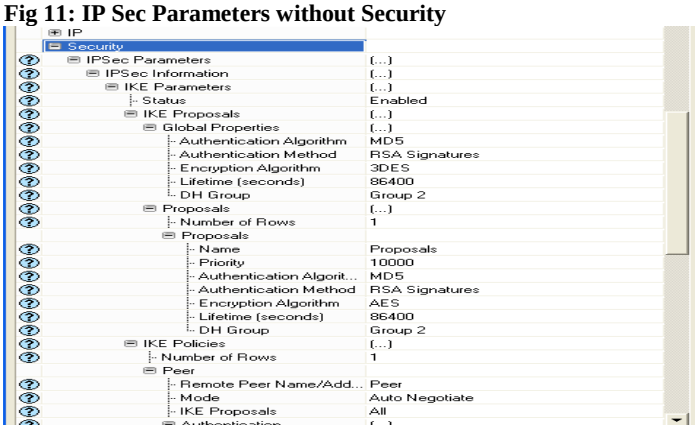

Fig 12: Parameter Associated with IP Sec

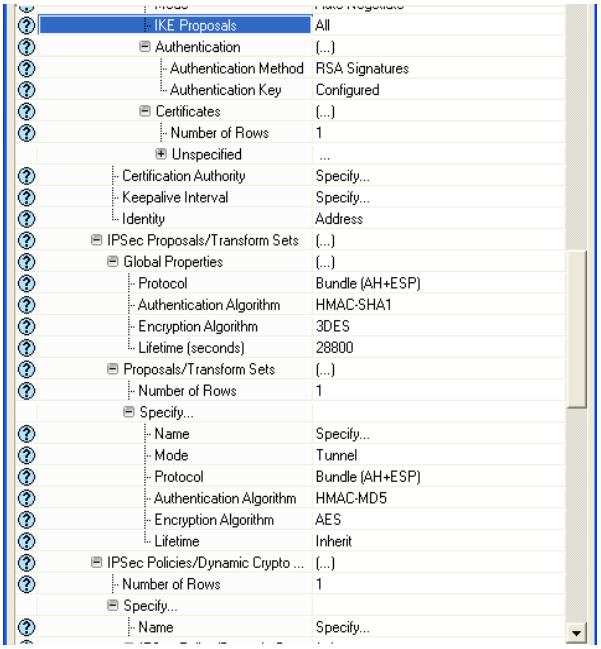

Fig 13: Parameter Associated with IP Sec (Con't)

9. RESULT AND ANALYSIS
AES Security

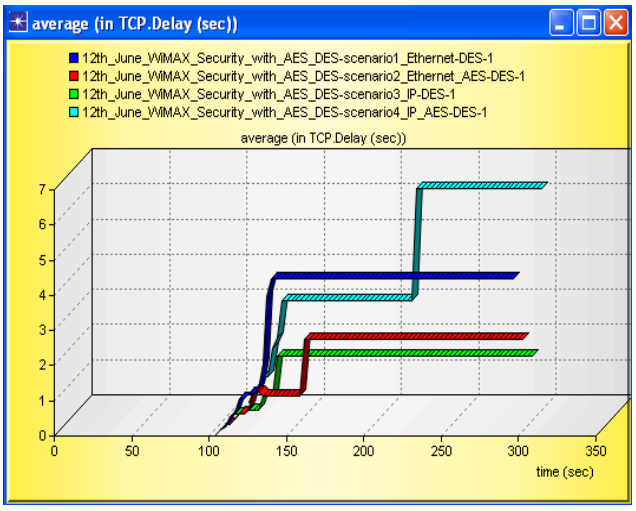

Fig 14: TCP Delays in Sec

We have estimated that downlaod respnse time in case of IP with AES security based network is high in comparasion to Ethernet based server. Result has reflected in **Figure 14.**

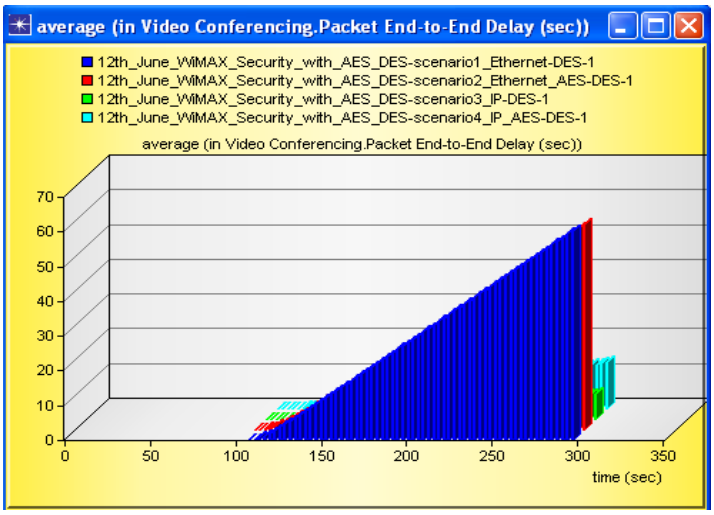

Fig 15: Packet End-to-End Delay

In video application the Packet End to End delay variation is same in case of Ethernet based server with and without AES security but in IP based network have more End-to-End delay as per **Figure 15.**

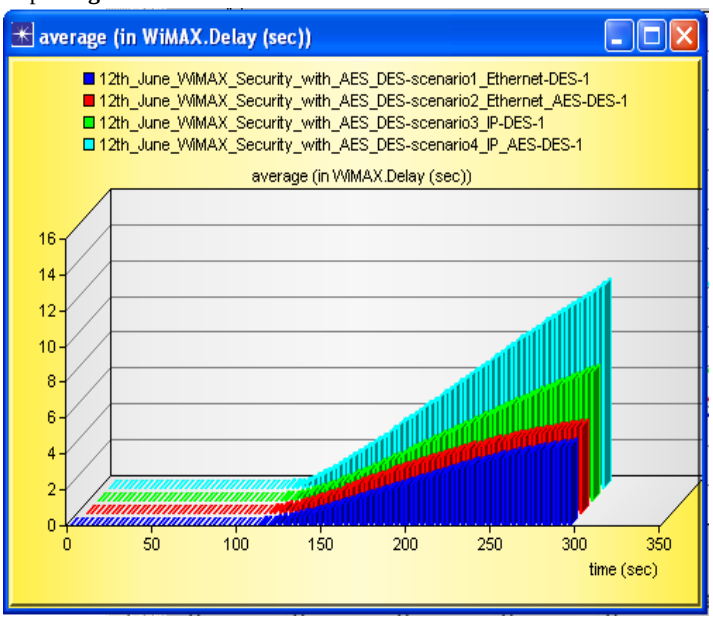

Fig 26 WiMAX Delay

From **Figure 16** we have estimated that the WiMAX delay is higher in IP based network than Ethernet based server with AES Security issue.

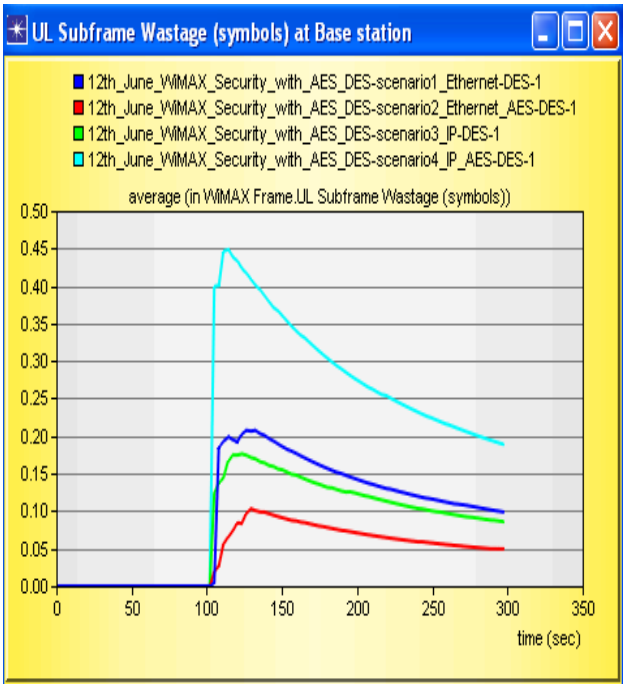

Fig 17: UL Subframe Wastage

This result given significant observation about AES security issues we have analyzed that with security IP (PP server) bsed network have higher UL subframe wastage then rest of scenario. (**Figure 17)**

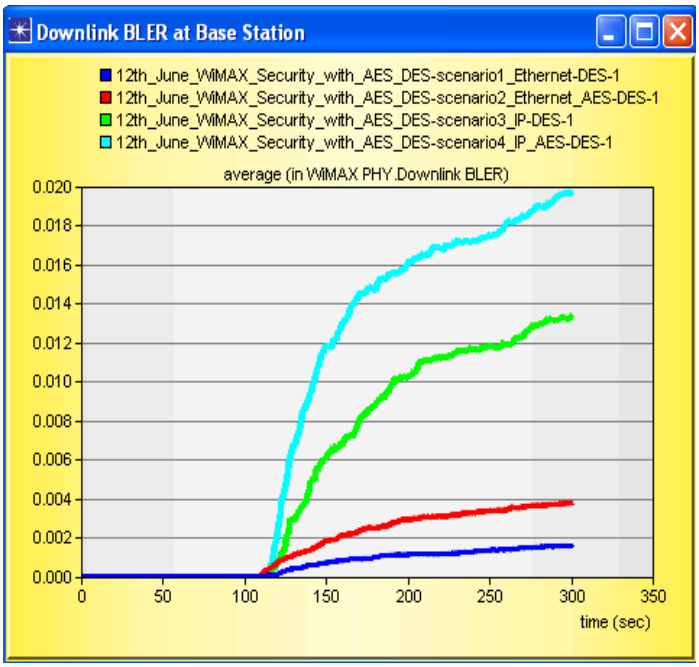

Fig 38: WiMAX PHY BLER

In above figure (**Figure 18)** we have estimated that BLER in case of IP based server with security have highest block level error rate.

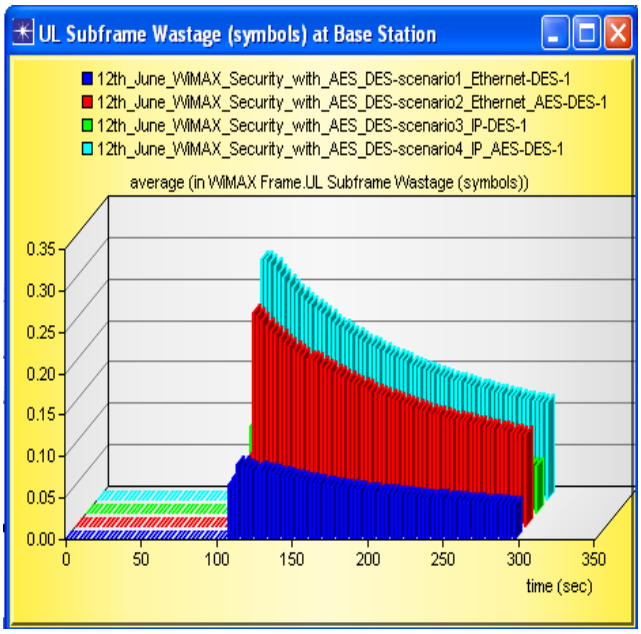

Fig 49: UL Subframe Wastage

When we applied security in all scenarios we analyzed that UL Subframe wastage is high comparison to without security. (**Figure 19)**.

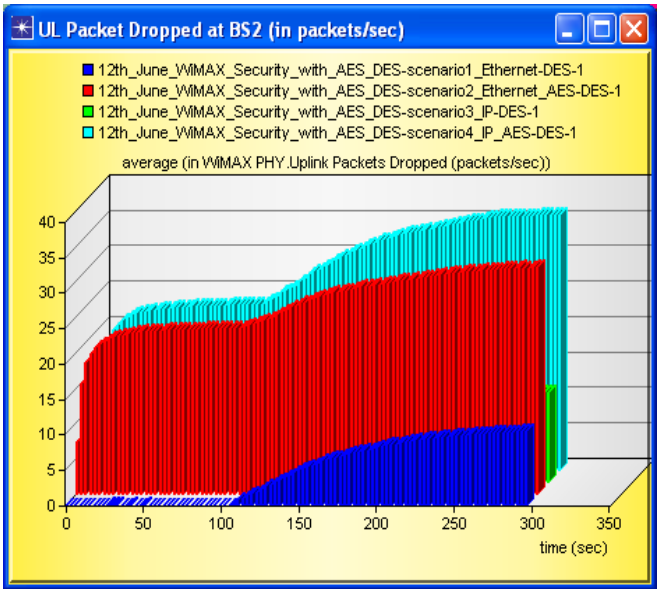

Fig 20: UL Packet Dropped

Above result given significant impact on the networks because in both type of networks when AES is not applied Packet dropped is very low (Maximum 5 Packet/Sec) and it is started after 100 Sec. When security will applied the Packets dropped started form initially and up to 100 Sec Packet dropped amount is 30 Packets/sec and after 100 Sec the amount is increase by 5 Packet and total dropped is 35 (30+ 5) with security and without security.(**Figure 20)**

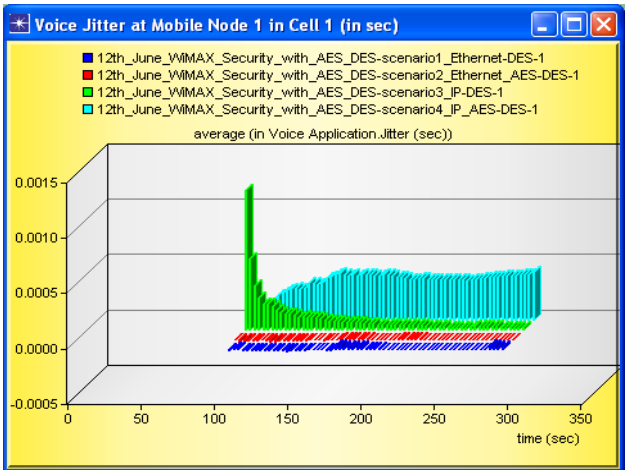

Fig-25: Voice Jitter

In above figure (**Figure 21)** we observed that packets variation in voice application is also effected more in case of IP based server networks.

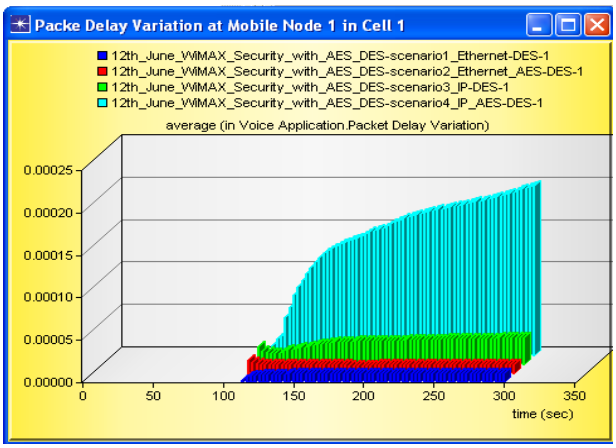

Fig 22: Packet delay Variation

When we have analyzed the packet delay variation at individual node in the case of IP with Security is again highest.(**Figure 22)**

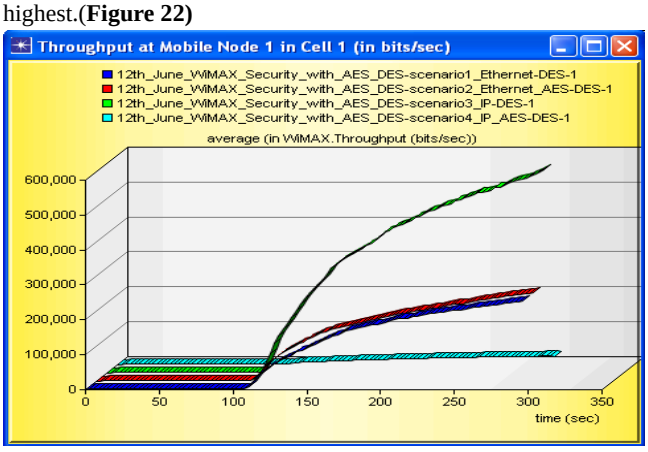

Fig 236: WiMAX Throughput

When we have estimated the throughput at Mobile Node Paper, In case of IP based server and link after security has been applied the throughput decrease very high due to secure packet transfer. Here again we have judged that the impact of security on Ethernet based server is very low. (**Figure23)**

10. CONCLUSION

In this paper, we describe the security issue between inter network with IKE management for traffic loads in WiMAX networks. We have considered all the possible scenario i.e ATM based and packet based simple network and with AES enabled network. We concluded that on the basis of all result there is tradeoff between throughput and i.e Packet based networks. So in our view we can able to pay more cost for secure network because all the required demand by users is good in packet based networks. So we conclude that packet based network is better performance as far as security concerns. If you see other face of networks basically we will pay less because in this scenario we are using current infrastructures and LBRRA is better choice in case of current user interface.

11. ACKNOWLEDGEMENT

The author would like that thank his guide Dr Upena D Dalal and ECED department, NIT, Surat (SVNIT), India. The authors also acknowledge the significant contribution of his parents (Shiva Shankar Jha and Yamuna Jha).

12. AUTHORS PROFILE

Rakesh Kumar Jha: Mr. Jha Rakesh presently is full time Research Scholar from S. V. National Institute of Technology, Surat, INDIA. He has completed his B.Tech. (Hon's in Electronics and Communication) from Bhopal and obtained M.Tech (Hon's in Wireless Communications) from NIT, Jalandhar, India. He have done live project in development and support both in Industries. He has published more than 20 International conferences and journal papers. His one concept related to Router of Wireless Communication has been accepted by ITU (International Telecommunication Union) in 2010. He has received Young Scientist Author award by ITU in 2010. He has received APAN fellowship in 2011. He is member of IEEE, GISFI and SIAM, International Association of Engineers (IAENG) and ACCS (Advance Computing and Communication Society). He is now pursuing PhD in S. V. National Institute of Technology, Surat, INDIA. Surat. His research interest's area is Wireless and Optical Communication (OPTI SYSTEM). Currently he is doing his research work in WiMAX and its Security issues. He is working on OPNET Modeler and Qualnet simulation tools for Wireless Communication.

Dr Upena D Dalal: Dr. (Mrs.) U. D. Dalal presently working as Associate Professor in Electronics Engineering Department of S. V. National Institute of Technology, Surat, INDIA. She has 19 years of academic experience. She completed her B.E. (Electronics) from SVRCET, Surat in 1991 and obtained M.E. (Electronics & Communications) from DDIT, Gujarat with Gold Medal. She is also awarded with 5th N.V. Gadadhar memorial Award by IETE. She has published many conference and journal papers at national and international level. She has guided many UG and PG projects, dissertations and seminars in the area of advance communication systems. She has completed Ph.D. in 2009

and guides 9 research scholars presently. Her book on "Wireless Communication" is published by Oxford University Press in July 2009. One more book edited by her and Dr Y P Kosta titled "WiMAX New Developments" is published by Inteh, Vienna, Austria. She is honored by "Rashtriya Gaurav Award" by India International Friendship Society. Recently she is received Best Technical Woman award by Divyabhaskar.

13. REFERENCES

[1] Md. Rezaul Karim Siddiqui, Sayed Mohammad Atiqur Rahman, "Security analysis of the WiMAX technology in Wireless Mesh networks", Thesis from Blekinge Institute of Technology (BTH), Karlskrona, Sweden, 2009, pp 42-46

[2] ILYAS, S. A, "WiMAX Standards and Security", 2008. London: CRC Press.

[3] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhammad, "Fundamentals of WiMAX Understanding Broadband Wireless Networking, 2007

[4] Seok-Yee Tang, "WiMAX Security and Quality of Service an End-to-End Prospective", 2010

[5] Rakesh jha,Upena D Dalal, "Location Based Performance of WiMAX Network for QoS with Optimal Base Stations (BS)"Wireless engineering and Technology(WET) journal by scientific research, Vol. 2, No.3, PP.135-145, July 2011

[6] Rakesh Jha, Upena D Dalal, "Security Analysis of WiMAX Network: With Misbehavior Node Attack" 2011 World Congress on Information and Communication Technologies, WICT-2011, IEEE Xplore, pp-397-404, Dec 2011

[7] Rakesh Jha, Upena D Dalal," WiMAX System Simulation and Performance Analysis under the Influence of Jamming", Scientific Journal, Volume -1,No-1,July 2010, pp-20-26

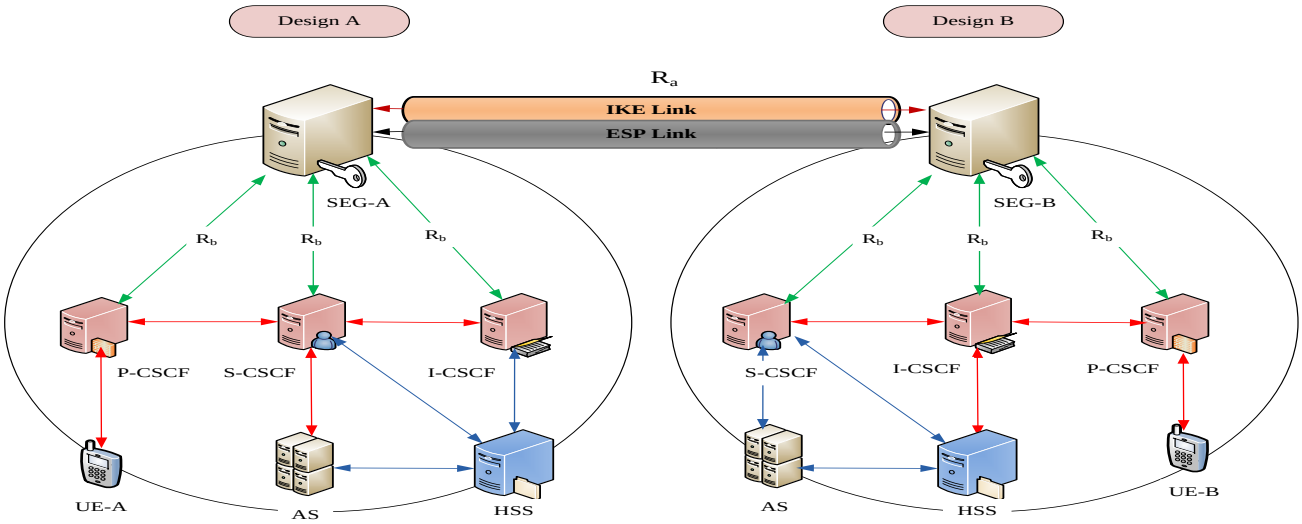

Fig 1: IKE for security issue