Comparative Analysis of MAC and HMAC-Sha3 using NS-2

Tanika Gupta
Student / C.S.E
LLRIET ,Moga
Punjab, India

Mehak Aggarwal
Associate professor / C.S.E
LLRIET ,Moga
Punjab, India

Mandeep Kumar
Assistant Professor / IT
FCET, Ferozepur
Punjab, India

ABSTRACT
Wireless Broadband offers tremendously fast and always on provide internet similar to ADSL and the user free from the fixed access areas and remove the hindrance of fixed access area for users. In order to achieve these features in formalized way was achieved for Wireless LAN and Wireless Metropolitan Area Networks with the advent of IEEE802.16 standards respectively from the beginning. The information is accessible for users in various areas because of that wireless network has become the major focus area as for as security matter is concerned .In this paper, we enhance the security levels by using HMAC in WiMax.

General Terms
Encryption, Decrytion, Ciphers.

Keywords
Wimax, MAC, HMAC,PHY,CS,

1. INTRODUCTION
WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way. WiMAX is a telecommuni--cation technology that provides wireless and broadband data transmission with high bandwidth and transmission rates between point-to-point links and full mobile cellular access. IEEE 802.16 supports fixed and nomadic nodes whereas IEEE802.16e the Mobile WiMAX standard derived from Fixed WiMAX supports mobile nodes.

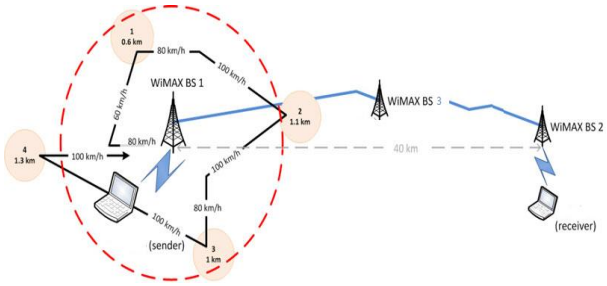

Fig 1: WiMAX supports mobile nodes.

WiMax has major realistic significance and strategic value as a standard facing to "the last kilometer" wireless broadband access as an alternative to cable and DSL.

WiMAX would operate similar to WiFi, but at higher speeds over greater distances and for a greater number of users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure. WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the WiFi Alliance is to 802.11. The name "WiMAX" was created by the **WiMAX Forum**, which was formed in June 2001 to promote conformity and interoperability of the standard, including the definition of predefined system profiles for commercial vendors. WiMAX was initially designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s[3] for fixed stations.

1.1 WiMAX MAC layer operation
1.2 Wimax Protocol
In order to understand WiMAX security issues, we first need to understand WiMAX architecture and how securities specifications are addressed in WiMAX. This section provides background and detailed information about WiMAX securities specifications in the security sub-layer.

1.3 IEEE 802.16 Protocol Architecture
The IEEE 802.16 protocol architecture is structured into two main layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer. MAC layer consists of three sub-layers. The first sub-layer is the Service Specific Convergence Sub-layer (CS), which maps higher level data services to MAC layer service flow and connections. The second sub-layer is Common Part Sub-layer (CPS), which is the core of the standard and is tightly integrated with the security sub-layer. This layer defines the rules and mechanisms for system access, bandwidth allocation and connection management.

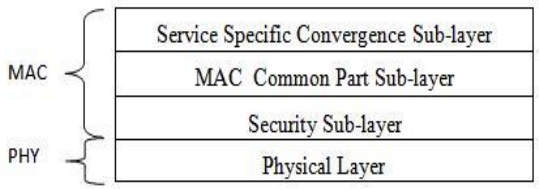

Fig:2 Wimax Protocol Stack

The MAC protocol data units are constructed in this sub-layer. The last sub-layer of MAC layer is the Security Sub-layer which lies between the MAC CPS and the PHY layer, addressing the authentication, key establishment and exchange, encryption and decryption of data exchanged between MAC and PHY layers. The PHY layer provides a two-way mapping between MAC protocol data units and the PHY layer frames received and transmitted through coding and modulation of radio frequency signals.

1.4 Wimax MAC layer
Transmission of data - reception of MAC Service Data Units, MSDUs from the layer above. It then aggregates and encapsulates them into MAC Protocol Data Units, MPDUs,

before passing them to the physical layer, PHY for transmission.

2. WIMAX ARCHITECTURE

WiMAX Architecture is designed and developed on all-IP platform with all packet technology and without any legacy circuit telephony. **Figure 3** presents WiMAX architecture. This IP-based WiMAX network architecture consists of three main sections, namely User Terminals, Access Service Network (ASN) and Connectivity Service Network (CNS)

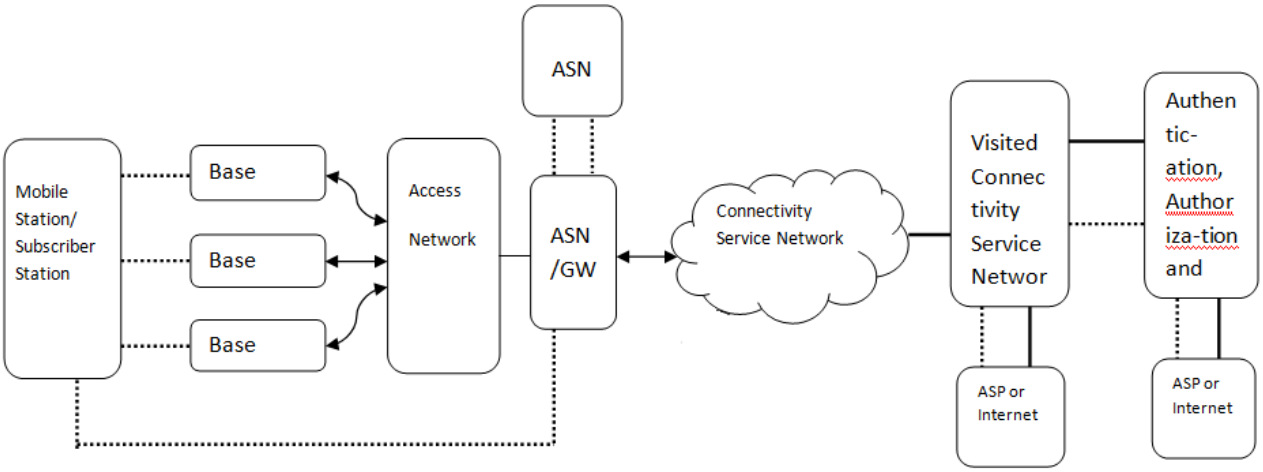

Fig 3: Wimax Network Architecture

2.1 Base station (BS)

The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micro mobility management functions.

2.2 Access service network gateway

The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management, and admission control, caching of subscriber profiles, and encryption keys also recommend email address.

2.3 Connectivity service network

The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services.

3. MESSAGE AUTHENTICATION CODE

In cryptography, **message authentication code** (often **MAC**) is a short piece of information to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin. A MAC is also called a keyed, cryptographic hash function is only one of the possible ways to generate MACs, accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC.

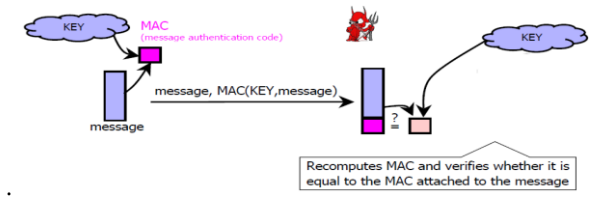

Fig:4 Authentication Without Encryption

The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content. The sender of a message runs it through a MAC algorithm to produce a MAC data tag.

3.1 Wimax MAC Protocol Data Unit

The completion of authentication and initial key exchange, data starts to flow between the BS and the SS by using the Traffic Encryption Keys (TEK) for encryption. Figure 5 shows this process. The Data Encryption Standard with Cipher Block Changing (DES-CBC) enciphers the MPDU payload field only leaving the header and the Cyclic Redundancy Check (CRC) without encryption in order to support diverse services. Once the security sub-layer generates an MPDU,it checks the Security Association (SA) associated with the current connection and obtains the Initialization Vector (IV). The MPDU IV is generated by XORing the SA IV with the synchronization field in the PHY frame header. The DES-CBC algorithm then encrypts the MPDU plaintext payload by using the generated MPDU IV and the authenticated TEK. To indicate that the payload in the MPDU is encrypted, the Encryption Control (EC) field of the MAC header is set to 1. The 2-bit Encryption Key Sequence (EKS) indicates which TEK is used.The CRC field is updated in accordance with the changes in both the payload and MAC header Construct MAC by applying a cryptographic hash function to message and key Could also use encryption instead of hashing, but…Hashing is faster than encryption in software Library code for hash functions widely available Can easily replace one hash function with another There used to be US export restrictions on encryption !Invented by Bellare, Canetti, and Krawczyk (1996) !Mandatory for IP security, also used in SSL/TLS.

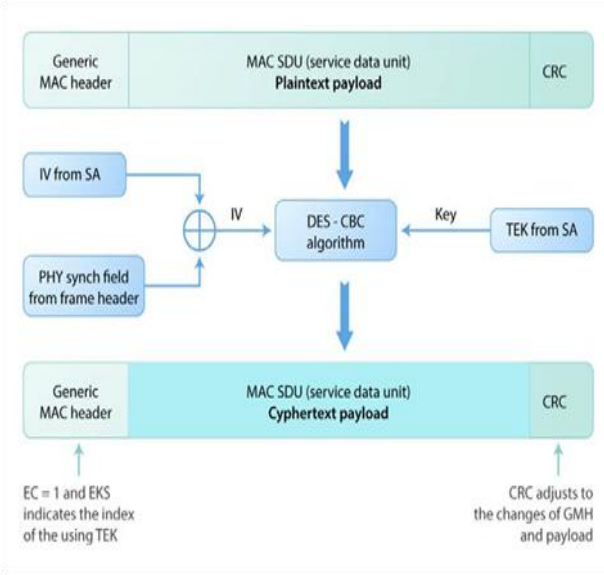

Fig 5: WiMAX encryption Process with MAC

4. HMAC-SHA3

Hashed Message Authentication Code (HMAC) for some message authentication and integrity control. 802.16e added the possibility of using CMAC as an alternative to HMAC. The HMAC keyed hash.The HMAC-Digest attribute, which is present in some PKM messages such as Key Request, Key Reply, Key Reject, etc. The HMAC Tuple is a TLV parameter used for some MAC management message authentications. The messages that can be authenticated with HMAC include DSx-REQ, DSx-ACK, REG-REQ, etc.

4.1 Structure of encryption HMAC

The HMAC Tuple is made of HMAC-Digest HMAC with **SHA-3,** on 256 bits, HMAC Key Sequence Number, on 4 bits, and a reserved field.

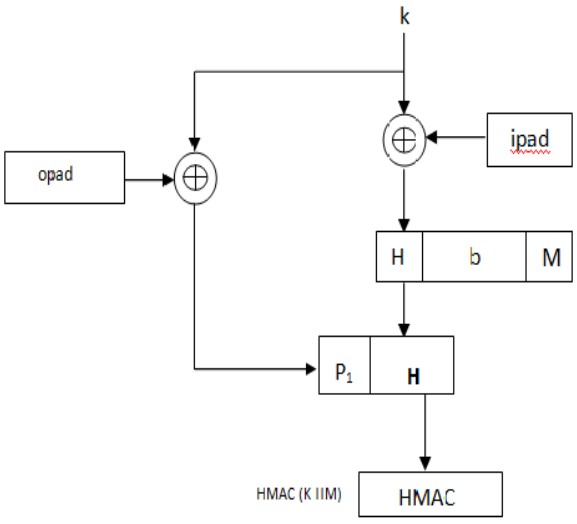

Fig:6 Structure of encryption HMAC

The HMAC Sequence Number in the HMAC Tuple is equal to the AK Sequence Number of the AK from which the HMAC_KEY_x was derived. Hash algorithm and key are used in both sender and receiver side to get the matching HMAC tages to prove that the data is authentic. HMAC use of crytographic hash function which is irreversible, so when we use HMAC from the sender side to encypt a message using the HMAC formula, then at the sender side . It is also more secure then sha3.

HMAC Algorithm Parameters and symbols:

M input message

B Block Size

H Embedded Hash Function

K Secret Key

Ipad Inner pad repeated in B times

Opad Outer pad repeated in B times

⊕ Exclusive or

II Concatenation

4.2 Structure of decryption HMAC

The receiver will use the hash function and the key to compute a value which should match with the hash value. Afterwards we Decrypt the cyphertext with the help of authentication Key and compute the HMAC on the plain text. if both values are equal then the decryption is accepted otherwise it will be rejected.

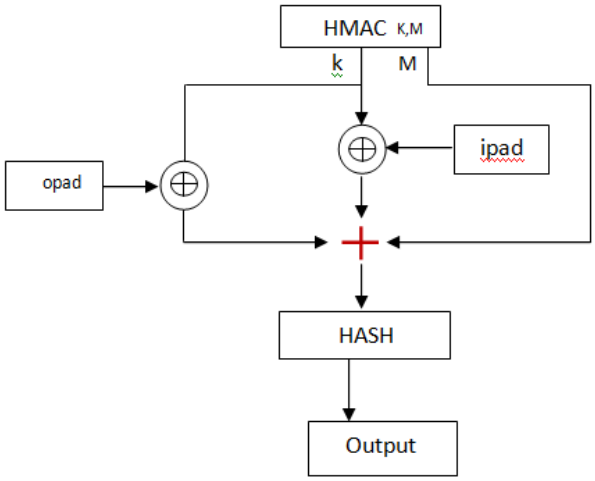

Fig:7 Structure of decryption HMAC

5. SIMULATION AND IMPLEMENTATION OF MAC AND HMAC-SHA3 IN WIMAX

In our research work, we have used HMAC-SHA3 Algorithm in Wimax to provide Cryptographic integrity. Our simulation environment is NS-2.34; here we have taken a test bed of 50 nodes. We have taken a parameter for this evaluation, Throughput. For better clearance of result and comparing it with data taken for MAC and HMAC-SHA-3, we have taken values for three different length of message keys i.e. 64,128,256 bits

5.1 Throughput

The Throughput is defined as the number of successfully received packets in a unit time and it represented in Kbps .throughput is calculated using .awk scripted which processes the trace file and produces the result.

In communication networks, such as Ethernet or packet radio, network throughput is the average of successful message

delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second or data packets per time slot. It can be calculated as maximum throughout, maximum theoretical throughput, maximum sustained throughput, peak throughput, normalized throughput.

It is defined as the total number of packets received at the destination per unit time. It is measured in Kbps.

$$Throughput=N/T;$$

N=total number of packets received

T=time taken

The figures 8,9 and 10 represent the values of throughput using HMAC-SHA3 in Wimax with 64, 128, 256 bit length of key.

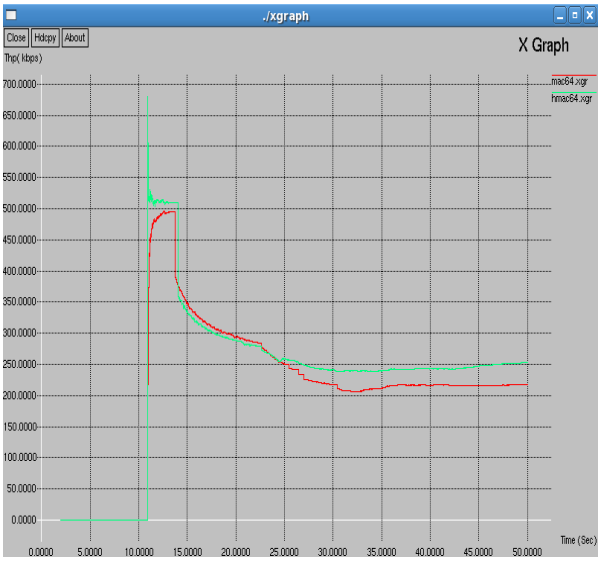

Fig 8 : Throughput using MAC and HMAC-SHA3 in wimax with 64 bit length Key

As shown in Fig:8 of throughput [Kbps] and pause time [sec]of MAC and HMAC-SHA3, comparison is done between the two algorithms at 64 bit key. According to the graph, MAC has lower throughput than HMAC-SHA3.

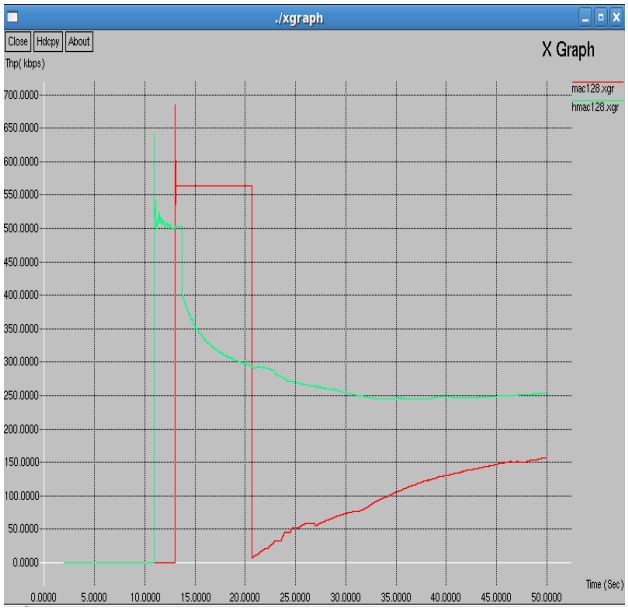

Fig 9: Throughput using MAC and HMAC-SHA3 in Wimax with 128 bit length key

As shown in Fig: 9 throughput [Kbps] and pause time [sec]of MAC and HMAC-SHA3, comparison is done between the two algorithms at 128 bit key. According to the graph, MAC has lower throughput than HMAC-SHA3.

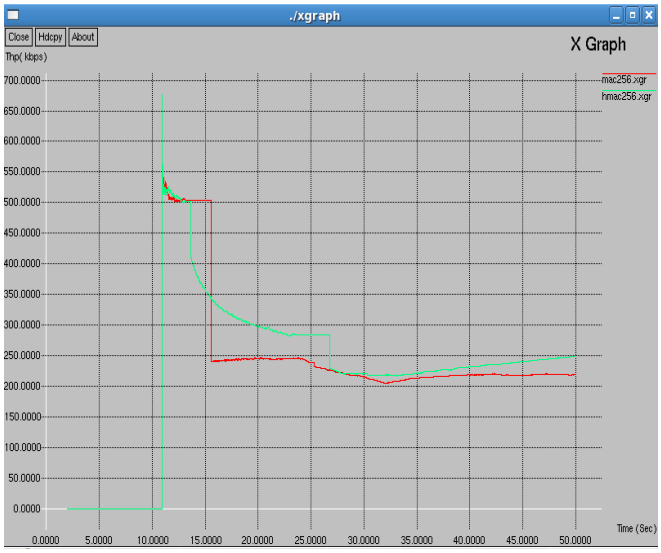

Fig 10: Throughput using MAC and HMAC-SHA3 1in Wimax with 256 bit length key

As shown in Fig: 10 throughput [Kbps] and pause time [sec] of MAC and HMAC-SHA3, comparison is done between the two algorithms at 256 bit key. According to the graph, MAC has lower throughput than HMAC-SHA3 .

We have compared throughput with HMAC-SHA3 in Wimax under similar conditions. we have found that HMAC-SHA3 is more secure than MAC and also it shows some improvement over MAC under specific conditions. These values are compared in following figure (Table:1).

Table 1: Comparison of Throughput with 3 different length of keys

Key Length	64 Bit	128Bit	256 Bit
MAC	218.28	157.43	219.29
HMAC-SHA3	253.39	253.10	248.79

5.2 Packet Delivery Ratio

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source. It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ration, the more complete and correct the routing protocol. 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. Route Change losses : is Defined as number of Lost Packet during Route Change. Since all Packet sent during Tdetect (time between moment in which link failure take place and instant in which link breakage detected)by node that detects link breakage will be lost. it is calculated as : Nlosses =X.Tdetect Nlosses are number of packet lost during route change X is packet sending rate Tdetect= RCL The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace _le. In general, PDR is defined as the ratio between the received packets by the destination and the generated packets by the source. Packet Delivery Ratio is calculated using .awk script which processes the trace _le and produces the result.

5.2.1 Packet delivery ratio :

the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

Number of packet receive / Number of packet send

If the pattern is matched with the line in the trace in the trace file specified action will be

performed.

In the END part final calculation is performed on the data obtained from the content part.

1. set the pattern and action for generated packets

2. set the pattern and action for received packets

3. Find the ratio between both

Table 2: Comparison of Packet delivery ratio with 3 different length of keys

Key Length	64 Bit	128Bit	256 Bit
MAC	0.7465	0.7071	0.8055
HMAC-SHA3	0.8017	0.8134	0.8425

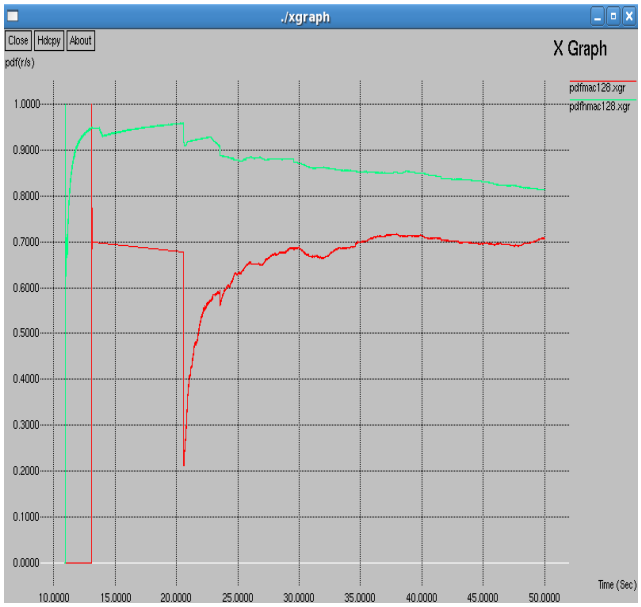

Fig 11 : Packet Delivery Fraction using MAC and HMAC-SHA3 in wimax with 64 bit length

As shown in Fig:11 of **Packet Delivery Fraction** [r/s] and pause time [sec]of MAC and HMAC-SHA3, comparison is done between the two algorithms at 64 bit key. According to the graph, MAC has lower **Packet Delivery Fraction** than HMAC-SHA3.

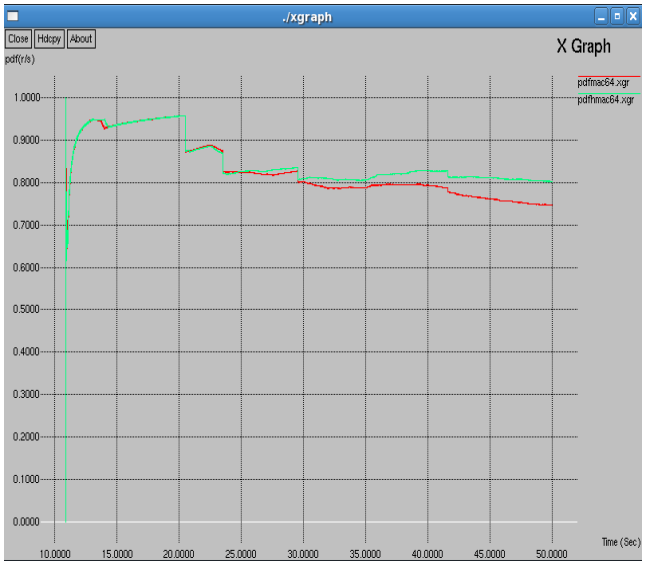

Fig 12 : Packet Delivery Fraction using MAC and HMAC-SHA3 in wimax with 128 bit length

As shown in Fig:12 of **Packet Delivery Fraction** [r/s] and pause time [sec]of MAC and HMAC-SHA3, comparison is done between the two algorithms at 128 bit key. According to the graph, MAC has lower **Packet Delivery Fraction** than HMAC-SHA3.

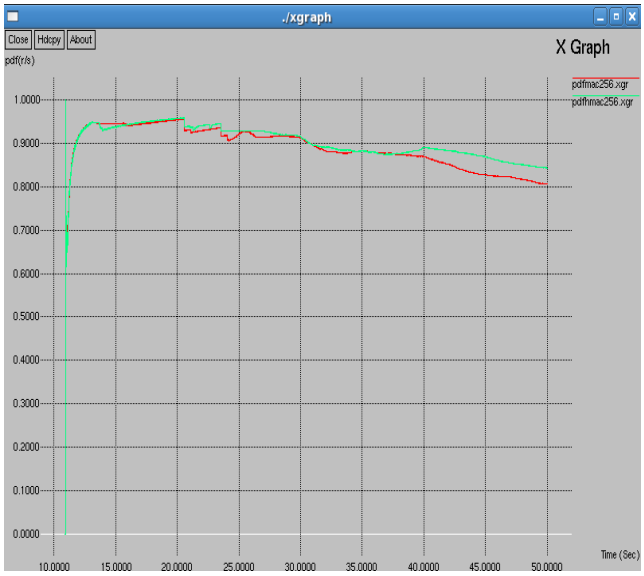

Fig 13: Packet Delivery Fraction using MAC and HMAC-SHA3 in wimax with 256 bit length

As shown in Fig:13 of **Packet Delivery Fraction** [r/s] and pause time [sec]of MAC and HMAC-SHA3, comparison is done between the two algorithms at 256 bit key. According to the graph, MAC has lower **Packet Delivery Fraction** than HMAC-SHA3.

6. CONCLUSION

Wimax has its own weaknesses but, it is still applicable in our daily life. While implementing and comparing MAC and HMAC-SHA3 algorithms based on throughput, Packet Delivery Fraction the performance of HMAC-SHA3 is better in terms of throughput , Packet Delivery Fraction also. While considering the future scope of the proposed work, more hash algorithms can be implemented on existing Wimax that will provide more security to the network. We have compared throughput and Packet Delivery Fraction with MAC in Wimax under similar conditions, we concluded that HMAC-SHA3 is more secure than MAC and also it shows some improvement over MAC under some specific conditions.

7. REFERENCES

[1] Syed Shabih Hasan, Mohammed Abdul Qadeer, "Security concerns in WiMAX", International Conference on Digital Object Identifier, 2009.

[2] Michel Barbeau, "WiMax/802.16 Threat analysis", Carleton University, 2005.

[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[4] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[6] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender