Department of Electrical and Electronic Engineering

THESIS REPORT ON

WiMAX SECURITY ANALYSIS

SUMMER 2011

Supervisor: Sadia Hamid Kazi

Co-supervisor: Rumana Rahman

Group members:

Nuha Saeed

Student ID: 08110102

Mahfuza Munira

Student ID: 08110039

Date: 11/08/11

Table of Contents: **Pg no.**

DECLARATION

We hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Signature of Supervisor

Signatures of Authors

ACKNOWLEDGMENTS

First of all we would like to thank the Almighty for all His blessings and kindness.

We are respectfully grateful to our supervisor Sadia Hamid Kazi for her guidance in every possible way through this exercise. She arranged all the facilities and the necessary supports, which were indispensable for our thesis.

We also thank our families and all our friends, especially those, who supported us with their valuable suggestion and encouragements.

Abstract

Worldwide Interoperability for Microwave Access (WiMAX) is a wireless metropolitan area network (WMAN) communications technology using the IEEE 802.16 standard. The original purpose of IEEE 802.16 technologies was to provide last-mile broadband wireless access as an alternative to cable, digital subscriber line (DSL). WiMAX provides some advanced features like scalability, mobility, high data rates, quality of service and security.

In our thesis we did some simulation to analysis the performance of PKMv1 and PKMv2. The number of lost frame is higher in case of PKMv2 that is because of the MAC overhead causes for the security issue. We also came to know that PKMv2 faces more delay than PKMv1 that is because of more secured connection causes long process of connection establishment , where as in PKMv1 only the SS/MS gets authenticated by BS but in PKMv2 both party share their X.509 certificates and get authenticated by each other. From the analysis and comparison we can see that may be PKMv2 gives us better security solution than PKMv1 but it still has some threats.

1. Threats in WiMAX

In order to understand WiMAX security issues, we first need to understand WiMAX architecture. The IEEE 802.16 protocol architecture is structured into two main layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer .The following threats affect all WiMAX systems:

1.1 Threats in Physical Layer

The following threats are seen in PHY layer:

RF Jamming

All wireless technologies are susceptible to RF jamming attacks. The threats arises from an adversary introducing a powerful RF signal to overwhelm the spectrum being used by the system, thus denying service to all wireless nodes within range of the interference. RF jamming is classified as a DoS attack. The risk associated with this threats is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009 WiMAX systems.[1]

Scrambling

Scrambling attacks are the precise injections of RF interference during the transmission of specific management messages. These attacks prevent proper network ranging and bandwidth allocations with the intent to degrade overall system performance. Scrambling attacks are more difficult to identify than jamming attacks because they are engaged for short time periods and are not a constant source of interference. The risk associated with this threat is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009. [3]

1.2 Threats in MAC Layer

The following threats are present in MAC layer:

Man-in-the Middle

Man-in-the-middle (MITM) attacks occur when an adversary deceives an SS/MS to appear as a legitimate BS while simultaneously deceiving a BS to appear as a legitimate SS/MS. This may allow an adversary to act as a pass-through for all communications and to inject malicious traffic into the communications stream. An adversary can perform an MITM attack by exploiting unprotected management messages during the initial network entry process. This is because the management messages that negotiate SS's/MS's security capabilities are not protected. If an adversary is able to impersonate a legitimate party to both the SS/MS and BS, an adversary could send malicious management messages and negotiate weaker security protection between the SS/MS and BS [Han06]. This weaker security protection may allow an adversary to eavesdrop and corrupt data communications. Mandating the use of AES-CCM in IEEE 802.16e-2005 and IEEE 802.16-2009 helps mitigate this attack because it appends a unique value to each data packet, which, in turn, prevents the MITM traffic relays between BS and SS/MS. IEEE 802.16-2004 does not offer adequate protection against MITM attacks.[4]

Eavesdropping

Eavesdropping occurs when an adversary uses a WiMAX traffic analyzer within the range of a BS and/or SS/MS. The adversary may monitor management message traffic to identify encryption ciphers, determine the footprint of the network, or conduct traffic analysis regarding specific WiMAX nodes. Data messages are subject to eavesdropping when encrypted using DES-CBC; using AES can provide robust data message confidentiality. The large operating range of WiMAX helps to shield eavesdroppers from detection; eavesdropping mitigation relies heavily on technical controls that protect the confidentiality and integrity of communications. The risk associated with eavesdropping management messages is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009. The risk associated with eavesdropping data messages is high for IEEE 802.16-2004 systems due to weak encryption. IEEE 802.16e-2005 and IEEE 802.16-2009 systems using AES protect their data messages from eavesdropping. [3]

DoS

Primarily, when a wimax network has no downlink or uplink data, it will enter either Sleep Mode or Idle Mode, both of which aim to trim down the power utilization of the mobile station. Upon the availability of data, the serving base station will awaken the mobile station. The mobile station then establishes a connection with the base station via initial ranging. Ranging parameters are then adjusted for the connection. Finally, the service flow is reactivated for data transfer, and the mobile station returns to the normal operation stage. Depending on whether the serving base station has the necessary information, the mobile station may need to carry out more signaling operations, such as basic capability negotiation, authentication and key management, re-registration, as well as IP connectivity reestablishment. Given the above signaling procedures, attackers may also launch similar signaling attacks to WiMax base station by triggering unnecessary state transitions that overload the base station with signal processing that leads to denial of service (DoS) attacks. [4]

2. WiMAX Standard Protocol Structure

WiMAX protocol structure is consists of MAC layer and physical layer.

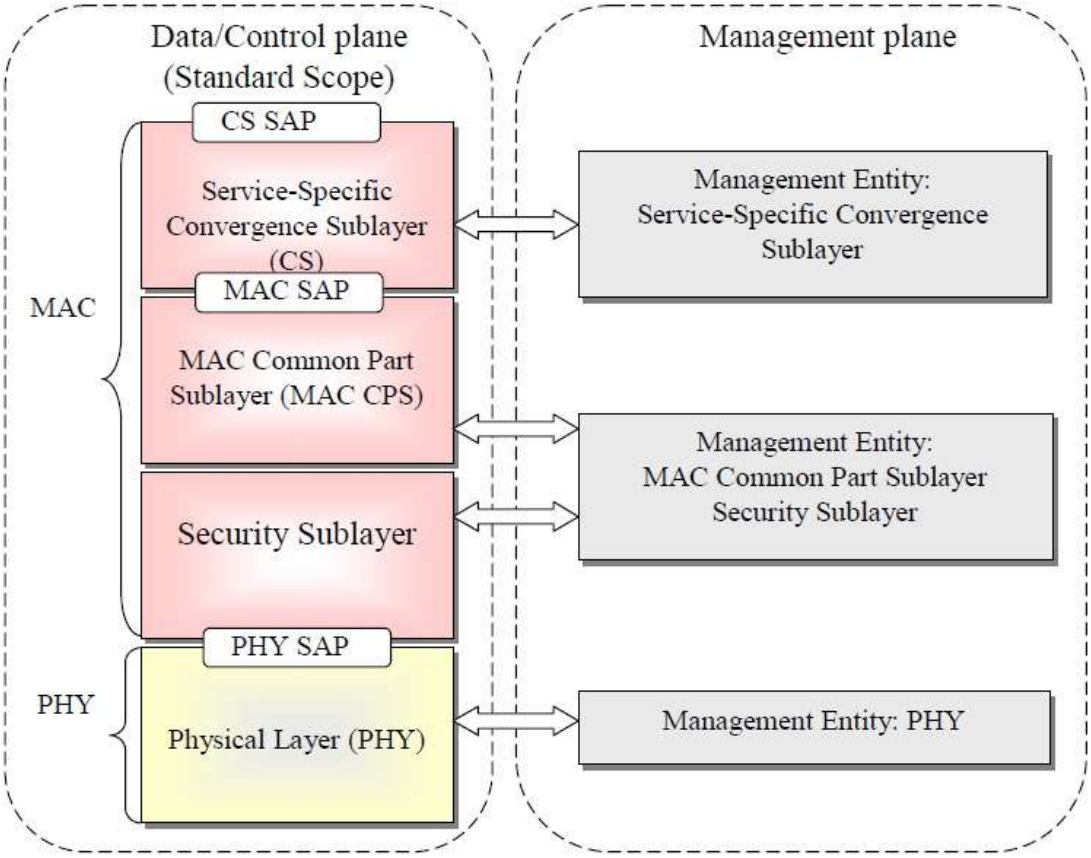


Figure 1: WiMAX Standard Protocol Structure [2]

MAC layer consists of three sub-layer, which are having following functions:

- **Service-Specific Convergence Sub layer(CS)**

The performance of CS is accepting higher layer protocol data units (PDU) and making classification of higher layer PDUs. Then process the higher layer PDUs based on the classification and deliver it to the appropriate MAC SAP. It also receives PDU from peer entity. [2]

- **MAC Common Part Sub Layer**

This layer provides MAC core functionality which involves with system access, bandwidth allocation, connection establishment and connection maintenance.

- **Security Sub Layer**

MAC security sub layer provide access control and confidentiality across the broadband wireless network through encryption and privacy key management.

3. WiMAX Security Features

WiMAX systems provide secure communications by performing three steps: authentication, key establishment, and data encryption. Figure 2 is a high-level overview of the security framework. The authentication procedure provides common keying material for the SS/MS and the BS and facilitates the secure exchange of data encryption keys that ensure the confidentiality of WiMAX data communications. The remainder of this section explains the basics of the WiMAX security framework, authentication, key establishment, and data encryption.

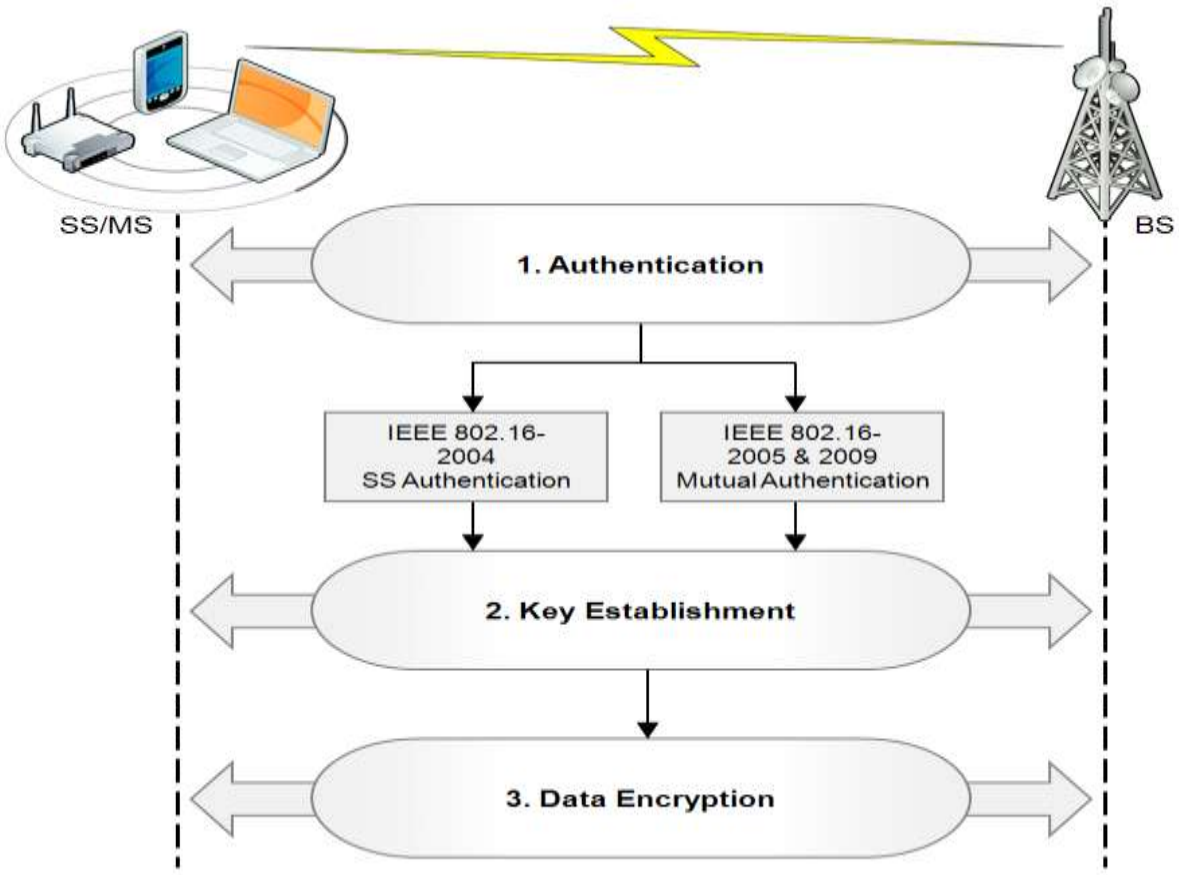


Figure 2: WiMAX Security Frame work [1]

4. Security Associations

A security association (SA) is a shared set of security parameters that a BS and its SS/MS use to facilitate secure communications. An SA defines the security parameters of a connection, i.e., encryption keys and algorithms. SAs fall into one of three categories: authorization, data (for unicast services), and group (for multicast services). Authorization SAs facilitate authentication and key establishment.

Authorization SAs contain the following attributes:

- **X.509 certificates.** X.509 digital certificates allow WiMAX communication components to validate one another. The manufacturer's certificate is used for

informational purposes, and the BS and SS/MS certificates contain the respective devices' public keys.

- **Authorization key (AK).** AKs are exchanged between the BS and SS/MS to authenticate one another prior to the traffic encryption key (TEK) exchange.
- **Key encryption key (KEK).** The KEK is used to encrypt TEKs during the TEK exchange.
- **Message authentication keys.** The message authentication keys validate the authenticity of key distribution messages during key establishment. These keys are also used to sign management messages to validate message authenticity.
- **Authorized data SA list.** Provided to the SS/MS by the BS, the authorized data SA list indicates which data encryption SAs the SS/MS is authorized to access.

Data SAs establish the parameters used to protect unicast data messages between BSs and SSs/MSs.[1]

A data SA contains the following security attributes:

- **SA identifier (SAID).** This unique 16-bit value identifies the SA to distinguish it from other SAs.
- **Encryption cipher to be employed.** The connection will use this encryption cipher definition to provide wireless link confidentiality.
- **Traffic encryption key (TEK).** TEKs are randomly generated by the BS and are used to encrypt WiMAX data messages.
- **Data encryption SA type indicator.** This indicator identifies the type of data SA. There are three types:

1) Primary SA. This SA is established as a unique connection for each SS/MS upon initialization with the BS.

2) Static SA. This SA secures the data messages and is generated for each service defined by the BS.

3) Dynamic SA. This SA is created and eliminated in response to the initiation and termination of specific service flows.

Group SAs contain the keying material used to secure multicast traffic.

Group SAs contains the following attributes:

- **Group traffic encryption key (GTEK).** This key is randomly generated by the BS and used to encrypt multicast traffic between a BS and SSs/MSs.
- **Group key encryption key (GKEK).** This key is also randomly generated by the BS and used to encrypt the GTEK sent in multicast messages between a BS and SSs/MSs.[1]

5. Authentication and Authorization

The IEEE 802.16 standard generally refers to authorization as the process of authenticating WiMAX nodes and granting them access to the network. The PKM protocol is the set of rules responsible for authentication and authorization to facilitate secure key distribution in WiMAX. PKM uses authorization SAs to authenticate system entities so that data and group encryption SAs can be established. PKM's authentication enforcement function provides the SS/MS and BS with identical AKs; each AK is then used to derive the message authentication keys and KEKs that facilitate the secure exchange of the TEKs. IEEE 802.16-2004 derives the AK using PKM version 1 (PKMv1), whereas IEEE 802.16e-2005 and IEEE 802.16-2009 derive the AK using PKMv2. This section reviews the procedures used in both PKMv1 and PKMv2.[1]

5.1 PKMv1

PKMv1 provides one-way authentication. Figure 3 illustrates the challenge-response verification scheme used in PKMv1-based authentication. The authorization process is initiated when the SS sends an authorization information message to the BS. Immediately following the authorization information message, the SS sends an authorization request to the BS, which contains the following information:

- The SS's unique X.509 certificate, which includes its RSA public key
- A description of the SS's supported cryptographic algorithms

- The primary SAID.

Next, the BS validates the SS's X.509 certificate, communicates the supported cryptographic algorithms and protocols, and activates an AK for the SS. Then the BS sends the SS an authorization reply message containing the following information:

- The activated AK, encrypted with the SS's public key
- The AK sequence number used to differentiate between successive generations of AKs
- The AK lifetime
- A list of SAIDs that the SS is authorized to access and their associated properties.

The reauthorization process is identical to the initial authorization process with the exception that the authorization information message is not re-sent.

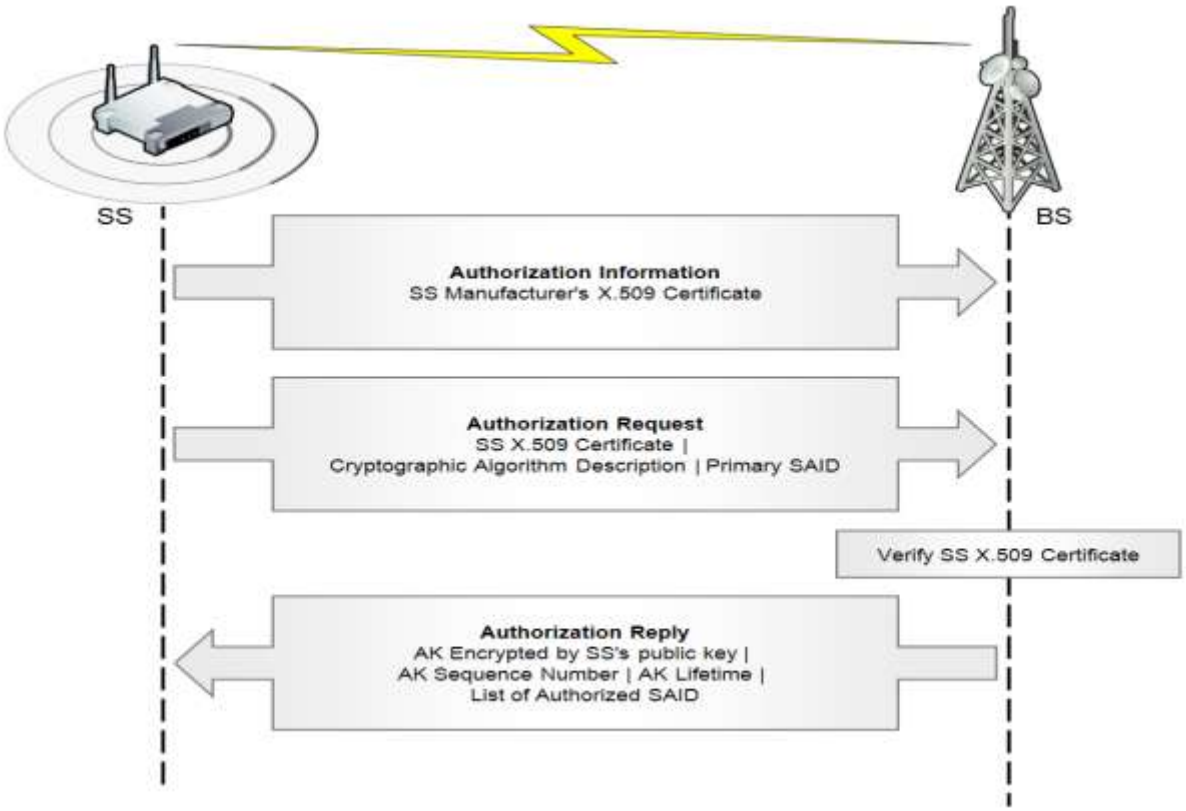


Figure 3: PKMv1 Authorization [1]

Flaws in PKMv1

Here authentication is one way. Only BS authenticates SS and no way for SS to authenticate BS. BS generates AK. SS does not generate AK, SS must trust BS for the generation of AK.[2]

PKMv2 provides mutual authentication between BS and SS.

Pro's of PKMv2

PKMv2 enhances PKMv1 by requiring mutual authentication between SS & BS. It has also more enhanced security features such as new key hierarchy for AK derivation and EAP. The PKMv2 key hierarchy defines the key category and the algorithms used to generate keys. The authentication and authorization processes generate source key materials. PkMv2 supports two authorization schemes:

- RSA-based authorization process
- EAP based authentication process

AK is derived from PAK and PMK in RSA and in EAP-based authorization procedure respectively.

5.2 PKMv2

IEEE 802.16e-2005 introduced PKMv2, which requires mutual authentication between the BS and the SS/MS. PKMv2 starts with what is known as RSA device mutual authentication. Figure 4 illustrates its challenge-response verification scheme. The exchange begins with the SS/MS sending an authorization information message containing the manufacturer X.509 certificate to the BS. [6]

The authorization information message is followed by an authorization request message sent from the SS/MS to the BS. It contains the following information:

- A 64-bit random number generated by the SS/MS
- The SS/MS's manufacturer-issued unique X.509 certificate
- A description of the SS/MS's supported cryptographic algorithms
- The primary SAID

Upon receipt of the authorization request message, the BS verifies the SS/MS X.509 certificate. If the certificate is valid, the BS sends an authorization reply message to the SS/MS containing the following:

- The 64-bit SS/MS generated random number sent in the authorization request message and another 64-bit random number generated by the BS19
- The 256-bit pre-PAK encrypted using the SS/MS's public key
- The Pre-PAK sequence number used to differentiate between successive generations of pre-PAKs
- The Pre-PAK lifetime
- A list of SAIDs that the SS/MS is authorized to access and their associated properties
- The BS's manufacturer-issued X.509 certificate
- The BS's signature provided by the BS's private key.

The SS/MS verifies the BS's X.509 certificate. If the certificate is valid, the BS and SS/MS proceed to the next authentication procedure to derive the AK.[1]

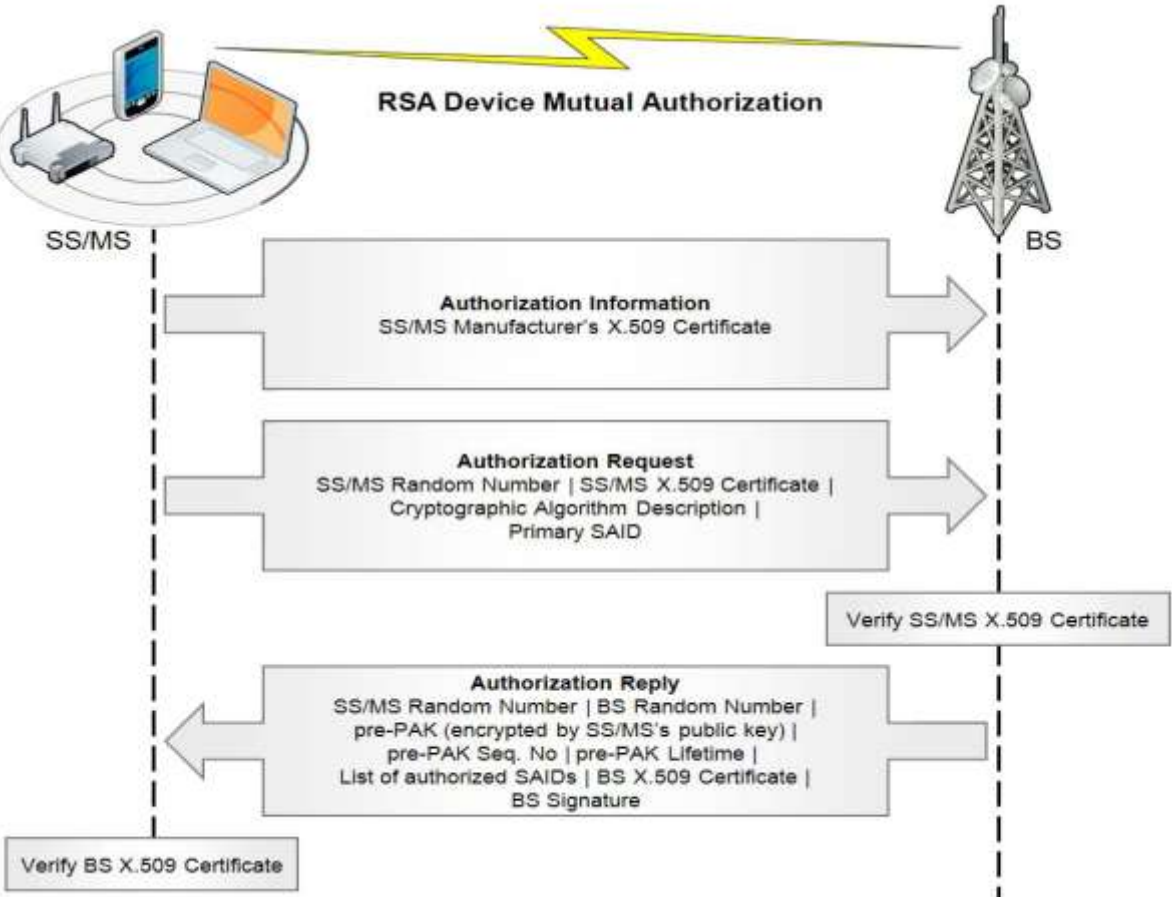


Figure 4: PKMv2 RSA Device Mutual Authorization [1]

After RSA device mutual authentication occurs, there are two options to derive the AK and complete authentication. One is called RSA-only authentication, and the other is known as EAP after RSA device mutual authorization.

In RSA-only authentication, both the BS and SS/MS symmetrically perform identical procedures on the pre-PAK to eventually derive the AK, as shown in Figure 5. The first procedure derives the 160-bit PAK from the pre-PAK, SS/MS media access control (MAC) address, and BS identifier. Next, the AK is derived from the PAK, the SS/MS MAC address, and the BS identifier.

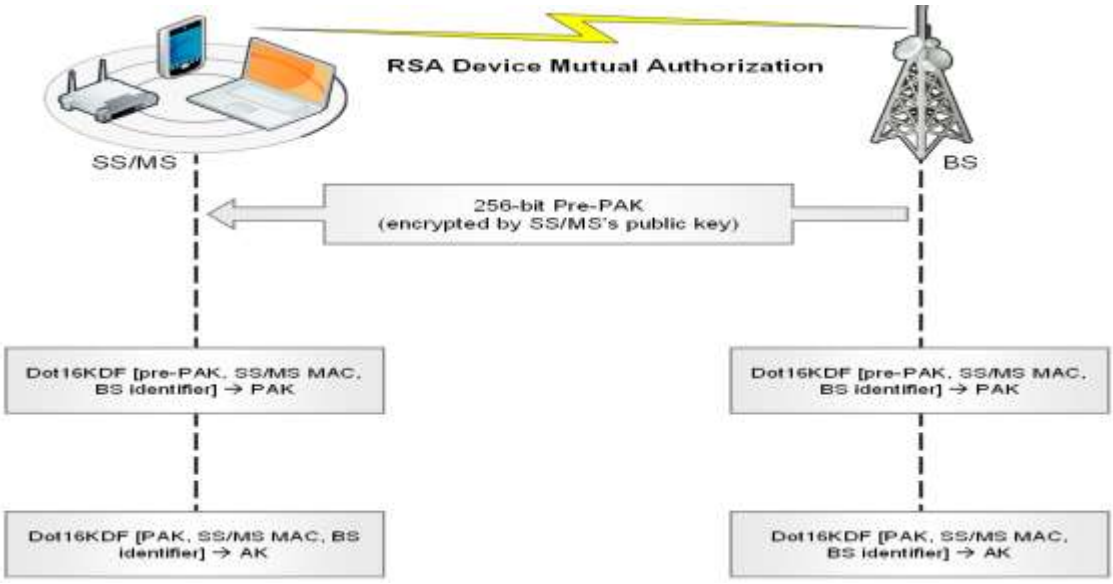


Figure 5: PKMv2 RSA-Only AK Derivation [1]

Figure 6 depicts the EAP after the *RSA* device mutual authorization procedure. The pre-PAK is delivered to the SS/MS and then used to derive the EAP integrity key (EIK) to secure the first EAP exchange. The first EAP exchange results in the production of a 512-bit master session key (MSK) that is disclosed to the authentication, authorization, and accounting (AAA) server, the BS, and the SS/MS. The BS and SS/MS truncate the MSK to 320 bits—160 bits for the pair wise master key (PMK) and 160 bits to create another EIK to protect an optional EAP user authentication procedure. The PMK, the SS/MS MAC address, and the BS identifier are then used to derive the AK. When using EAP after RSA device mutual authorization, device mutual authentication only takes place during initial network entry. For network reentry or re-authentication, only EAP authentication is required. [4]

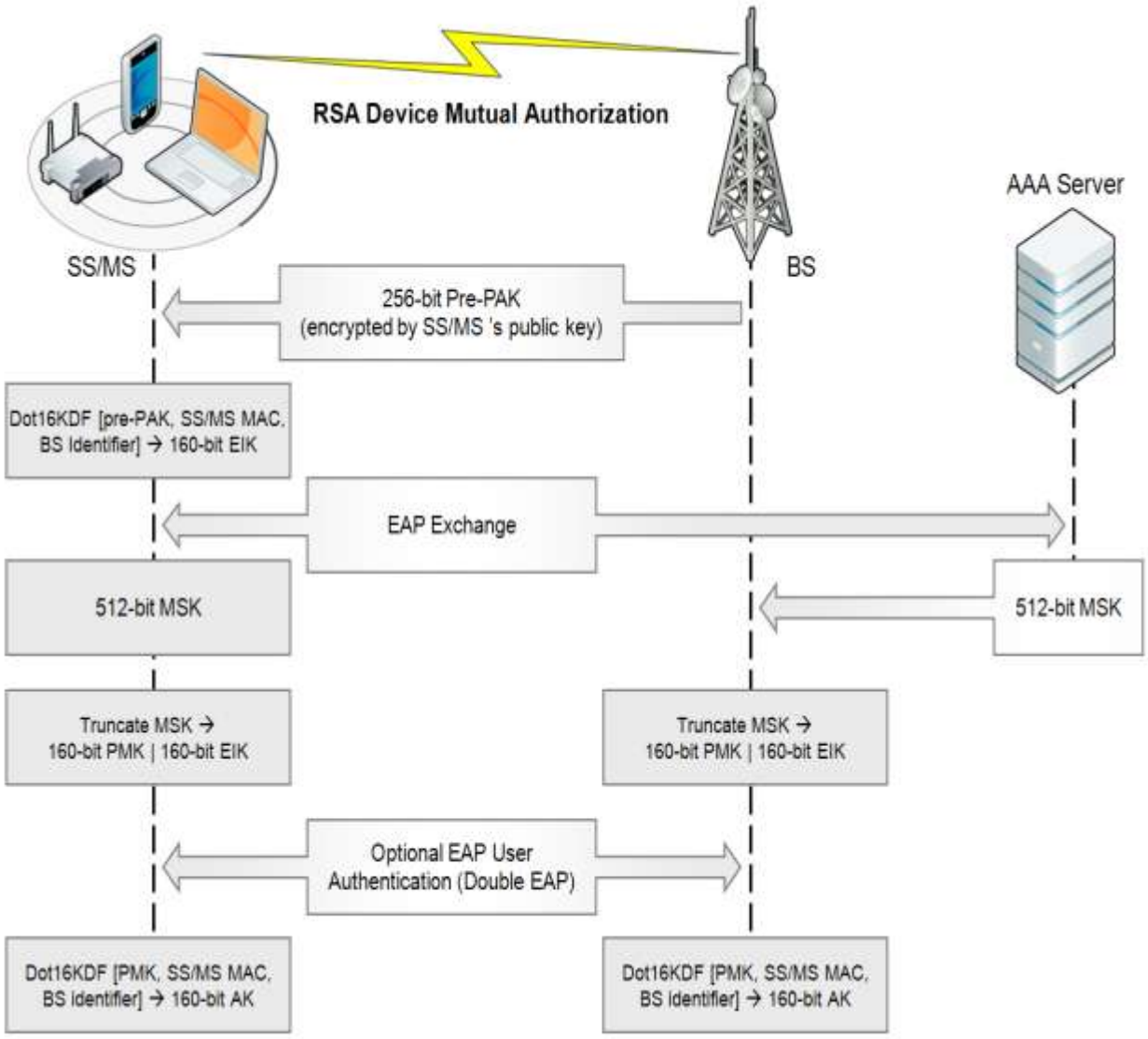


Figure 6: EAP after RSA Device Mutual Authorization [1]

5.3 Theoretical Comparison Between PKMv1 and PKMv2

PKMv1	PKMv2
Only BS authorizes SS/MS	Both BS and SS/MS authorizes each other
Single process	Runs two types of process – RSA based – EAP based
Vulnerable to DoS and MITM attacks	Mostly prevents DoS and MITM attacks

6. Encryption Key Establishment

Once authentication is complete, the BS and SS/MS share an activated AK. PKM then uses the 160-bit AK to derive the 128-bit KEK and the 160-bit message authentication keys, which are used to facilitate a secure exchange of TEKs.[1] The secure TEK exchange uses a three-way handshake between the BS and the SS/MS, as illustrated in Figure 7.

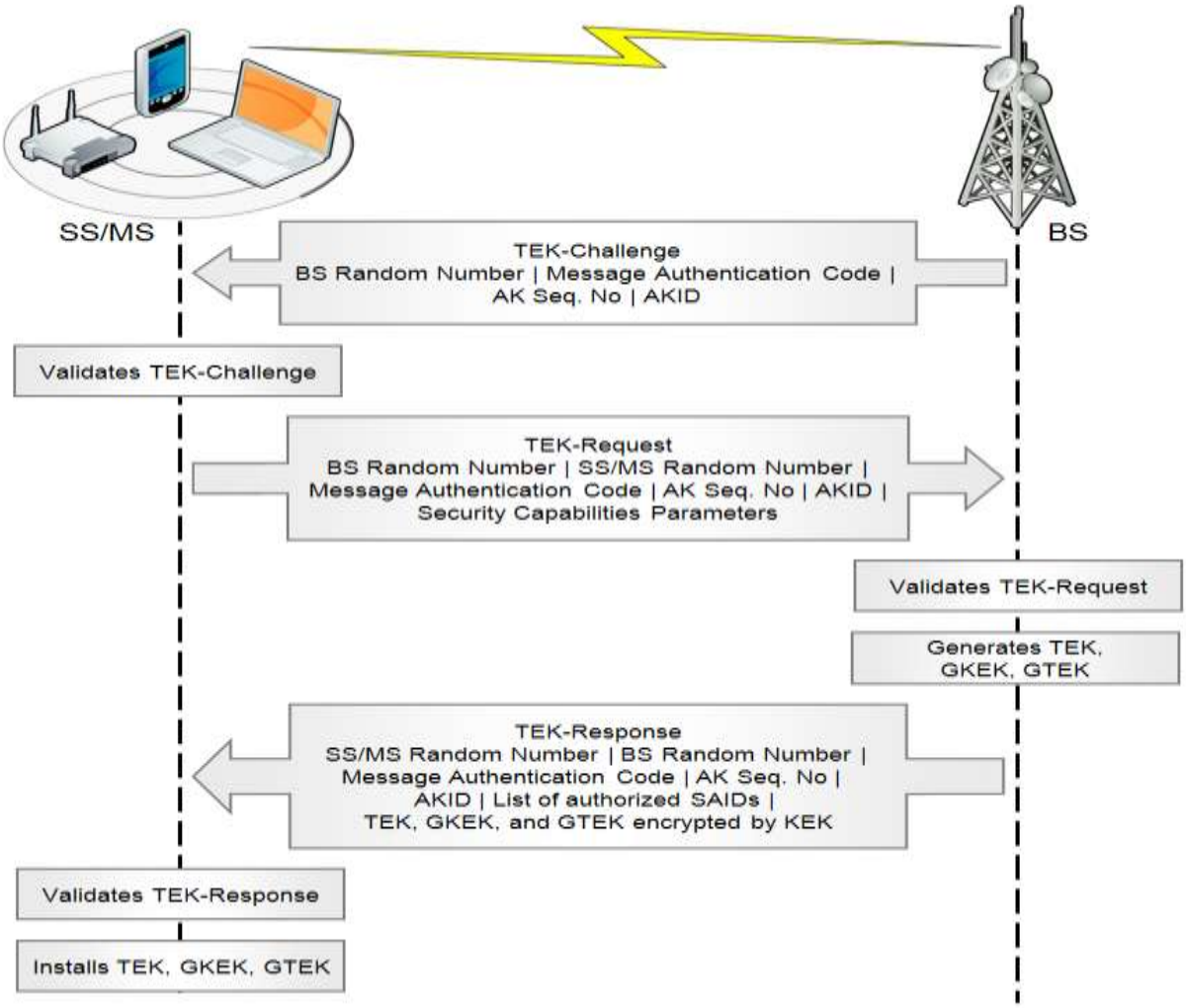


Figure 7: TEK Three-Way Handshake [1]

The first step in this procedure is the TEK-Challenge sent from the BS to the SS/MS. The TEK-Challenge is sent during initial network entry or during reauthorization. The TEK-Challenge includes the following attributes:

- **BS random number.** This number is attached to the TEK-Challenge to prevent replay attacks by validating message freshness.
- **Message authentication code.** These validate data authenticity of the key distribution messages sent from the BS to the SS/MS.
- **AK sequence number and AK identifier (AKID).** These attributes identify which AK is used for the TEK exchange.

Upon receipt of the TEK-Challenge, the SS/MS validates the authenticity of the TEK-Challenge using the message authentication keys. After the TEK-Challenge has been validated, the SS/MS then sends the TEK-Request to the BS, which contains the following attributes:

- **BS and SS/MS random numbers.** In addition to sending back the BS random number from the TEK-Challenge, the SS/MS attaches its own random value.
- **Message authentication code.** These validate data authenticity of the key distribution messages sent from the SS/MS to the BS.
- **AK sequence number and AKID.** These identify which AK is used for the TEK exchange
- **Security capabilities parameters.** These describe the security capabilities of the SS/MS, including supported cryptographic suites. During initial network entry, the TEK-Request will also include a request for SA descriptors to identify the primary, static, and dynamic SAs that the SS/MS is authorized to access.

Upon receipt of the TEK-Request, the BS verifies that the BS random number matches the number sent in the TEK-Challenge and validates the message authentication keys. The BS next confirms that the AKID refers to an available AK and that the security capabilities parameters provided by the SS/MS are supported. Once the TEK-Request is validated, the BS will generate two TEKs, along with the GKEK and the GTEK.[3]

The BS then sends the TEK-Response to the SS/MS, which contains the following attributes:

- **BS and SS/MS random number.** The BS attaches the BS random number generated in the TEK-Challenge and the SS/MS random number generated in the TEK-Request.
- **Message authentication code.** These validate data authenticity for the key distribution messages sent from the BS to the SS/MS.
- **AK sequence number and AKID.** These attributes identify which AK is used for the TEK exchange.
- **List of authorized SAIDs.** This is the list of primary, static, and dynamic SAs that the SS/MS is authorized to access.

- **TEKs, GKEK, and GTEK.** Using the KEK derived from the AK, the BS encrypts the two TEKs, the GKEK, and the GTEK. These keys include all of the required keying material needed to facilitate secure communications between the BS and SS/MS.

Upon receipt of the TEK-Response, the SS/MS will ensure the BS random number matches the value given in the TEK-Challenge and that the SS/MS random number matches the value delivered in the TEK-Request. The SS/MS will then validate the message authentication keys. Once validation is complete, the SS/MS will install the appropriate TEKs, GTEK, and GKEK, and secure communications can begin.

In the case of an MS performing a handover to a new BS, the TEK-Response message also includes TEK, GTEK, and GKEK parameters of the previously serving BS to reduce latency associated with renewing SAs.[4]

7. Data Encryption

WiMAX MAC layer encrypts only data messages not management messages. It checks the SA associated with the current connection and acquires the initialization vector (IV). Then encrypt the MPDU plaintext payload by employing the generated MPDU IV and

the authenticated TEKs. To indicate the payload in the MPDU is encrypted, it sets Encryption Control (EC) field of the MAC header to 1.Here, 2 bit encryption key sequence is used to indicate which TEK is used. Finally it updates the CRC field in accordance with changes in both the payload and MAC header. [2]

7.1 MPDU

In MPDU encryption process, the summation of IV from SA and PHY synch field from frame header produce IV. By using DES-CBC algorithm IV, TEK from SA and plaintext payload produce cyphertext payload.

The process of MPDU encryption process is given below:

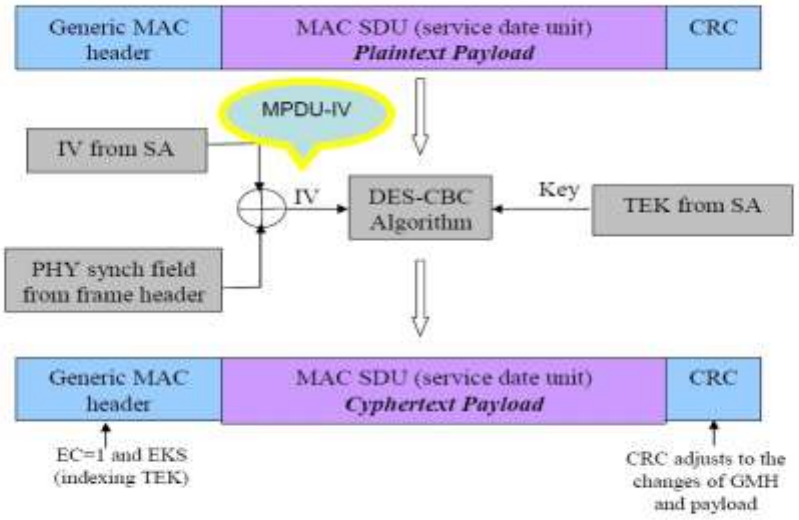


Figure 8: Encryption Process [2]

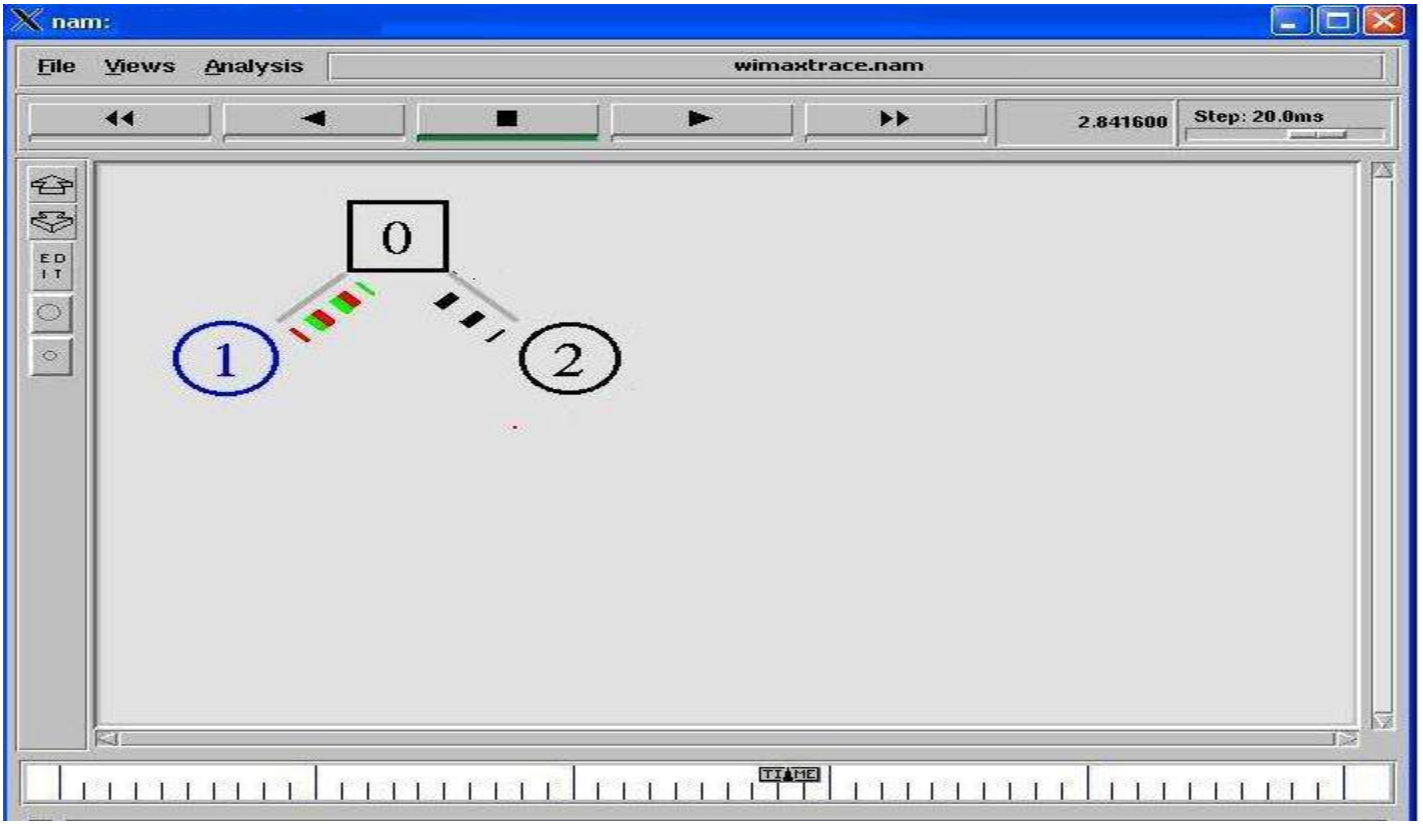
8. Simulation

In our thesis we did some simulation using NS 2.29 with WiMAX patch to analyze the performance of PKMv1 and PKMv2. The scenario we used consist of one IEEE 802.16e based BS outdoor unit (ODU), one indoor unit (IDU) and two SSs, where the BSODU and SSs are wireless devices and BS-IDU acts as a gateway for the BS-ODU

unit. A network management system (NMS) and the authentication, authorization, and accounting (AAA) severs are running on the BS-IDU unit. The system capacity BS is around 15 Mbps.[5]

- System Parameters

Network	IEEE 802.16e
Frequency Specification	3.5Ghz operating freq. 7Mhz bandwidth
Frame Specification	1500 bytes Pkt. Size, TCP packet



9. Analysis

9.1 Comparison of Output

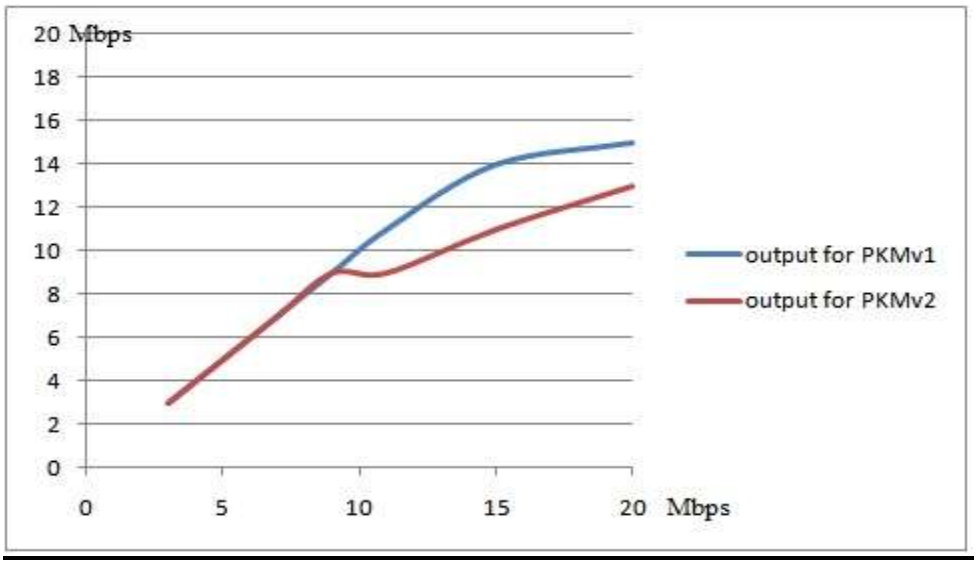


Figure 9: Throughput performance comparison of PKMv1 & PKMv2

It is a comparison of input vs. output curve for PKMv1 and PKMv2. Here we can see the output rate of PKMv2 is lower than PKMv1. That is because of the MAC overhead causes for the security issue. But there is a limitation in the size of packet over a wireless network. So the MAC overhead causes the packet size goes out of range, and the output rate goes steady near to 15 Mbps because of the capacity of BS.

9.2 Comparison of Dropped Frames

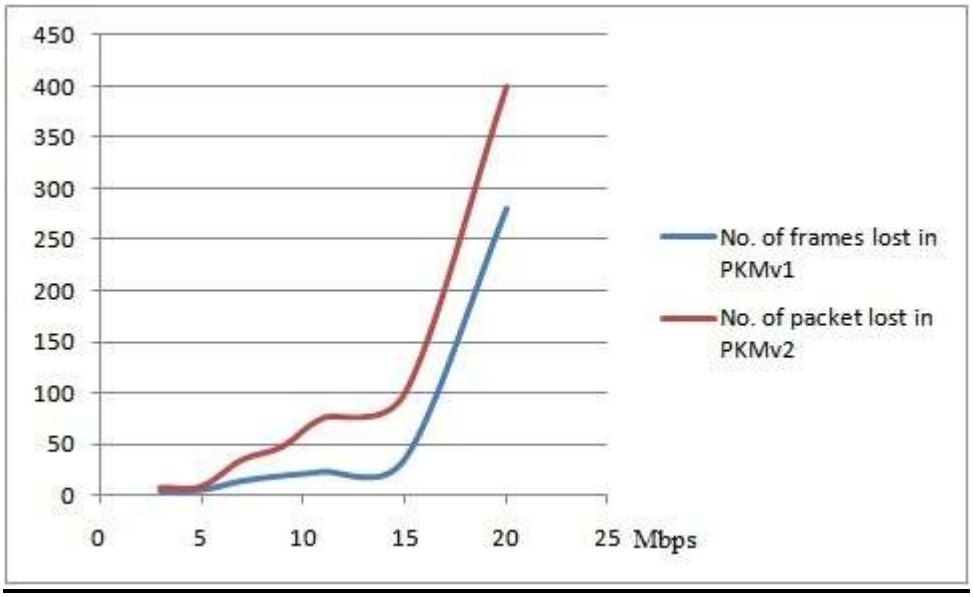


Figure 10: No. of packet dropped performance comparison of PKMv1 & PKMv2

Here we can see the curve of input vs. no. of lost frames for PKMv1 and PKMv2 and the number of lost frame is higher in case of PKMv2.That is because of the MAC overhead causes for the security issue and it also produces higher no. of packets. But there is a limitation in the size of packet over an wireless network. So the MAC overhead causes the packet size go out of range and as the number of packets goes higher the more packets get lost as there are limited space in buffer and when it goes out of the capacity of BS which is 15 Mbps, highest no. of packets get lost, so we can observe those spikes in the graph.

9.3 Comparison of Latency

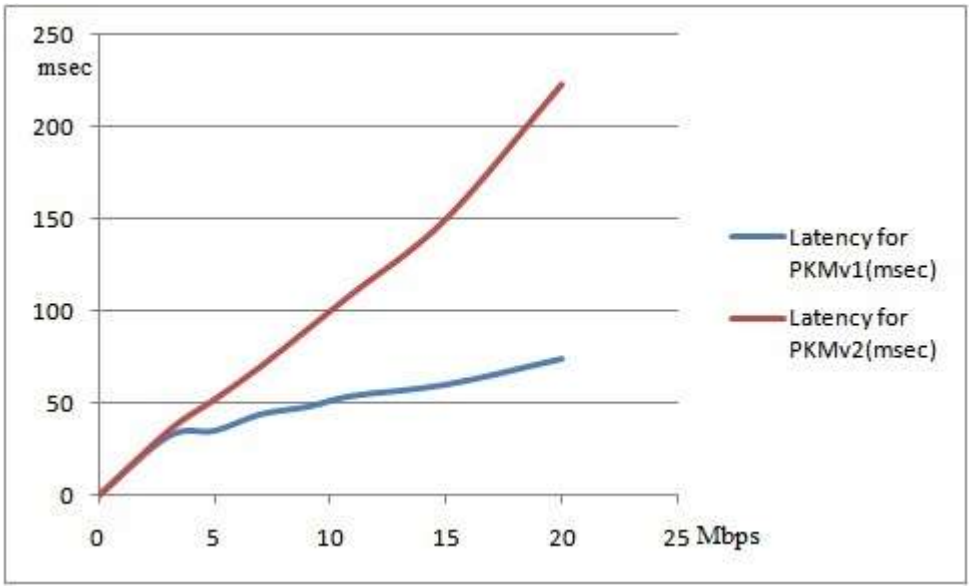


Figure 11: Latency performance comparison of PKMv1 & PKMv2

Here we can see the graph of input vs. latency in PKMv1 & PKMv2.we can easily say seeing the graph that PKMv2 faces more delay than PKMv1.that is because of more secured connection causes long process of connection establishment. Where as in PKMv1 only the SS/MS gets authenticated by BS, in PKMv2 both party share their X.509 certificates and get authenticated by each other. Moreover in PKMv2 process to secure the EAP exchange it uses EIK, which takes more time to be exchanged between SS, BS and AAA and to be derived.

10. Performance Based Comparison

PKMv1	PKMv2
Higher output rate	Lower output rate
Lower no. of lost frames	Higher no. of lost frames
Lower latency	Higher latency
No MAC overhead	MAC overhead
Faster connection	Slower connection
Less secured	More secured

Based on the analysis if we compare the performance of PKMv1 and PKMv2 then we can say although PKMv2 gives better security solution but it degrades the performance.

11. Solution

Our goal is to propose some possible solution to upgrade the performance of PKMv2 while at the same time it will give the same security to WiMAX network. Our 1st suggestion is to use timestamp in space of random nonce number. Time stamp allows tracking progress over time. So it can at the same time prevent replay attack as well as upgrade the performance of PKMv2 by reducing overhead of MAC header. Then next we can avoid encrypting SS address which is the MAC of SS, then BS also doesn't have to decrypt it which saves time. Moreover an encrypted SS address doesn't ensure more secured connection anyway. Our next suggestion is to avoid including SSID. The encryption by SS's public key already guarantees that the message is for SS only. Thus we can reduce the overload of MAC header of PKMv2 and upgrade its performance as well as the security.

12. Future Work

Our proposed suggestions can be tested using simulation tools like NS2 and if the test result shows that PKMv2 is able to give a better performance in the suggested way along with the security features then we can expect for a better secured connection for WiMAX than we are having now.

References

[1] Guide to Security for WiMAX Technologies (Draft); Karen Scarfone,Cyrus Tibbs,Matthew Sexton; NIST Special Publication 800-127; September 2009

[2] WiMAX Security: Privacy Key Management; Nirwan Ansari; 2007 Sendai International Workshop on Network Security and Wireless Communications; 24th January,2007

[3] A Journey on WiMAX and its Security Issues; Rakesh kumar Jha et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4) , 2010, 256-263

[4] WiMAX security and quality of service: an end-to-end perspective / edited by Seok-Yee Tang, Peter Muller, and Hamid Sharif; ISBN 978-0-470-72197-1

[5] http://www.virtualbox.prg/wiki/downloads

[6] http://www.freewimaxinfo.com