Key Management Protocol/Technique for IEEE 802.16 Mesh Networks

Developed By:

Muhammad Bakhsh

(188-FAS/MSCS/F04)

Muhammad Javed Iqbal

(203-FAS/MSCS/F04)

Supervised by

Mr. Mata-Ur-Rehman

Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad
2008

بسم الله الرحمن الرحيم

Dedicated to ONE

Who has all the names, and who does not need any name

A thesis submitted to the

Department of Computer Science

International Islamic University Islamabad
As a partial fulfillment of requirements for the award of
The degree of

MS in Computer Science

Declaration

We hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that we have developed the protocol and the accompanied report entirely on the basis of our collective efforts and under the sincere guidance of our supervisor Mr. Mata-Ur-Rehman. If any part of this project is proved to be copied out from any source or found to be reproduction of some other project, we shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Muhammad Bakhsh
(188-FAS/MSCS/F04)

Javed

Muhammad Javed Iqbal
(203-FAS/MSCS/F04)

International Islamic University
Islamabad

Dated 20th August 2008

Final Approval

It is certified that the research work presented in this thesis, entitled "Key Management Protocol/Technique for IEEE 802.16 mesh networks" is carried out by Muhammad Bakhsh RegNo: 188-FAS/MSCS/F04 and Muhammad Javed Iqbal RegNo: 203-FAS/MSCS/F04.

Committee

External Examiner

Dr. M. A. Ansari
Head Department of Computer Science
Federal Urdu University of Science, Arts and
Technology Islamabad

Internal Examiner

Dr. Mohammad Sher
Chairman Department of Computer Sciences
International Islamic University Islamabad

Supervisor

Mr. Mata-Ur-Rehman
Assistant Professor
International Islamic University Islamabad

Acknowledgement

We are very thankful to Almighty Allah, the most beneficent, the most merciful and the most gracious, for enhancing our courage for the completion of this work successfully. It is matter of great honor and pleasure for us to express our ineffable gratitude and profound indebtedness to *Dr. Mohammad Sher* for his kind supervision valuable suggestions and professional activities and inexhaustible energy to steer forth the students. We also appreciate efforts and cooperation of management of Department of Computer Sciences, International Islamic University Islamabad, Pakistan, that made it possible for us to complete our research. We are also greatly obliged to our supervisor *Mr. Mata-Ur-Rehman*, for his keen interest, guidance and moral support. We also express our thanks to Dr. Faizan ur Rehman , Zia Ahmed Khan Senior Instructors NIPA , Mr. Zeshan Shafi and Qutubuddin who helped us whenever needed.

Words are lacking to express our humble obligation to our parents whose hands always rise in prayers for our success. Lastly, we thank all our family members and friends who helped us during our study.

Muhammad Bakhsh
Muhammad Javed Iqbal

Project in Brief

Project Title:	**Key Management Protocol/Technique for IEEE 802.16 Mesh Networks**
Undertaken By:	**Muhammad Bakhsh** **Muhammad Javed Iqbal**
Supervised By:	**Mr. Mata-Ur-Rehman**
Start Date:	**November 2007**
Completion Date:	**June 2008**
Tools and Technologies:	**Java Programming Language**
Documentation Tools:	**MS word, MS Excel**
Operating System:	**MS Windows XP Professional**
System Used:	**Pentium 4, 1.73 GHz**

Abstract

In IEEE802.16 standard WIMAX is an evolving technology that is used for the broadband wireless access. Since this wireless technology is based on IEEE 802.16, which is a standard for Wireless Metropolitan Area Networks (WMANs). It was initially designed to deal with the "last mile" broadband connectivity for connecting networks together at a higher data rate. This facility can be an in-expensive one for homes, and businesses enterprises users. There were many security threats that the users can face. Security of WiMAX mesh is a hot issue these days in wireless communication especially in mesh networks. Possible threats exist like Replay Attack, DoS Attack, Jump forward Attack and BS/SS masquerading etc. Because of these security threats a secured authentication and key management protocol is proposed to solve the said security problems along with key issuance and management.

Thus the main objective the thesis is to study the WIMAX authentication and key management protocol, security architecture, encryption schemes used, study of limitations while implementing this protocol in mesh mode and so as to overcome the limitations in authentication and key management processes by introducing a new authentication and key management protocol for mesh networks.

Tables of Contents

Chapter # **Contents** **Page #**

List of Figures

List of Tables

1. Introduction

1. Introduction

Wireless communication is the transfer of information over a distance without the use of wires .The distances may be short (a few meters as in case of television remote control) or very long (like phone calls). When this context is clear the term is often simply called wireless. Wireless communications is generally considered to be a branch of telecommunications.

It is a matter of common observation that wired networks do not motivate service providers and users , however wireless access networks are more encouraging . this is because better structure ,speed and cost effectiveness. Such networks can be modified conveniently for the incoming subscribers as and when they grow. Wireless networks are more appealing in contrast to wired networks where most of monetary and nonmonetary inputs are to be made during the out set of deployment [19].

Such wireless installations are as wide spread as the wireless technologies are present today world .In this perspective every wireless technology is framed to achieve specific usage objectives:

1. Personal Area Networks (PANs)
2. Local Area Networks (LANs)
3. Metropolitan Area Networks (MANs)
4. Wide Area Networks (WANs)

The output , cost and other complexities of wireless networks expand from PAN's to WAN's . several implementations of the networks can be found but table1 presents only some well established networks.

Type	IEEE Standard	Commercial Name	Data rate	Range	Applications
PANs	802.15.1	Bluetooth	2Mb/s	100 m	Device-to-device, peer-to-peer communication
	802.15.3	UWB	Up to 50 Mb/s	10 m	
	802.15.4	Zigbee	250 Kb/s	10 m	
	802.15.4a		20 Kb/s	75 m	
LANs	802.11b	WiFi	11 Mb/s	100 m	Home, educational and enterprise networks, etc.
	802.11a		54 Mb/s	30 m	
	802.11g		54 Mb/s	100 m	
MANs	802.16a	WIMAX	Up to 75 Mb/s	50 km	Backhaul for hotspots, E1/T1 level services, portable and last mile broadband access
	802.16d		Up to 75 Mb/s	50 km	
	802.16e		Up to 15 Mb/s	5-15km	
	802.20	MBWA	1 Mbp/s	100 m	Mobile metropolitan wide services

Table 1: Wireless Networks

The above table does not include all the 802.11 and 802.16 extensions. some well known extensions of the wireless standard are 2G (GSM based), 2.5G (GPRS based) 3G (UMTS, CDMA 2000, EDGE) mobile wireless networks and satellite-based communication networks.

Common examples of wireless include:

1. Radio Services
2. Cellular telephones.
3. Global Positioning System (GPS)
4. Cordless computer peripherals.
5. Cordless telephone sets.
6. Satellite television

This generally provides easy service to laptop users , who often move from place to place. Similarly this applies to mobile configurations/wireless networks . some of the uses of wireless technology includes:

1. To reach at long distance which con not be covered through traditional cabling,
2. To overcome physical hurdles in the path of cables.
3. To incorporate feedback loops and linkages in case of breakdown.
4. To establish workable or timely subscribers.
5. This technology used in a place where cabling is financially impractical.

The IEEE paves the path of growing norms. Figure 1 shows some wireless standards for Wireless Local Area Networks (Wireless LANs), Wireless Personal Area Networks (Wireless PANs), and Wireless Metropolitan Area Networks (Wireless MANs) etc[18].

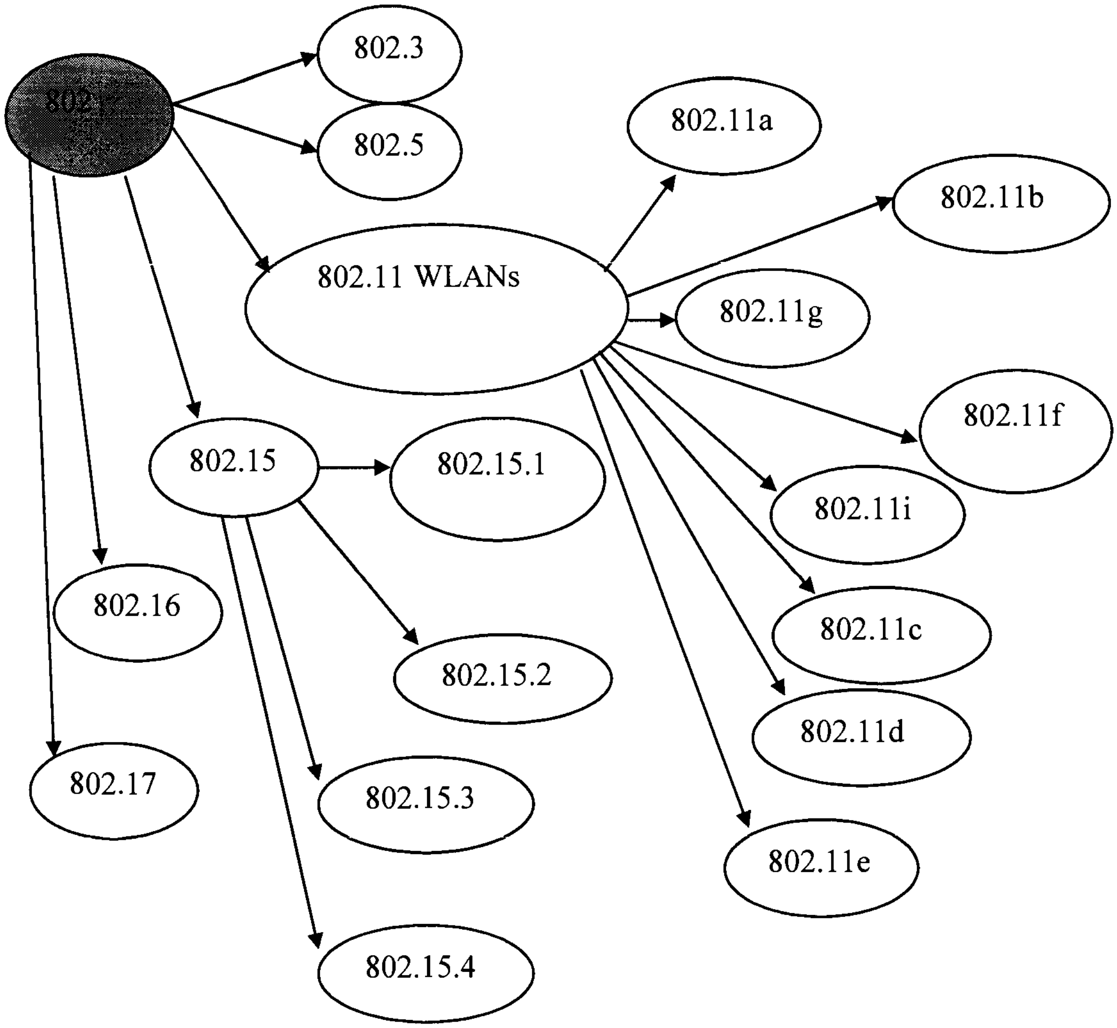

Figure 1: Wireless Standards Overview

1.1 WIMAX

When we think about the wireless broadband service then the name of WIMAX comes in mind which support fixed , portable , nomadic and mobile access .

WIMAX is a technology based on the 802.16 standard and specially designed for the metropolitan area networks. this technology bridges the gap between wireless LAN's and MAN's. the technology provides the wireless alternative for the broadband service in the remote/rural areas , which can not have access to wired broadband service.

When we talk about the features of the WIMAX which includes cost effectiveness and better bandwidth management. Last mile problem is also solved. If we see in future perspective , this technology give higher data rate through which more than one services are embedded in a single connection. Its bandwidth management is better than wifi. 802.16 MAC supports two modes of working i.e. PMP and Mesh.

1.1.1 Operation Modes of 802.16

IEEE 802.16 works in two modes

1. Point to Multipoint Mode(PMP)
2. Mesh Mode

1.1.1.1 PMP Mode

The operation of WIMAX in PMP mode is shown in the figure 1. In this mode the communication/link between the base station and the subscribers are handled through sectorized antenna.

If we consider the traffic flow in case of PMP mode then it should be in two way either from BS to SS of from SS to BS. if the traffic flows from BS to SS then it is called downlink and the reverse case is called uplink. Uplink deals with requests from the subscribers and downlink is a service from the BS.

Multiplexing schemes used by the WIMAX are FDM, TDM, OFDMA etc . In case of the frequency division multiplexing, uplink and downlink connections are maintained simultaneously for all the subscribers but in case of time division multiplexing ,multiple connections can be devided into time slots.

Generally, downlink traffic is broadcasted but in case of uplink bandwidth is shared among the subscribers. Bandwidth management is done by considering the class of service provided to the subscribers.

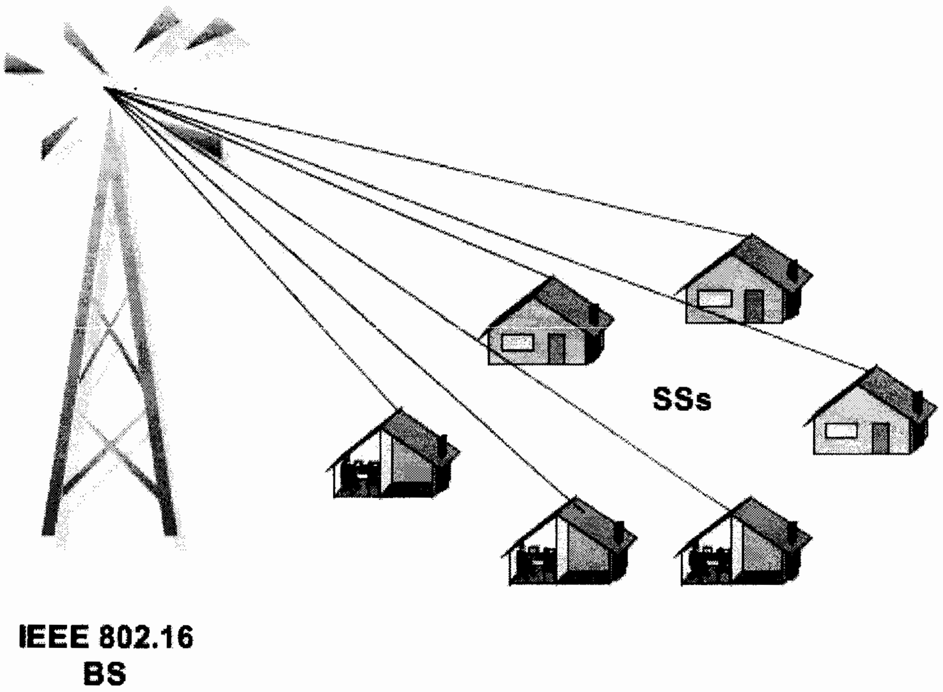

Figure 2: Point-to-Multipoint Mode

1.1.1.2. Mesh Mode

In addition to the PMP mode, mesh mode in WIMAX is more complex in a sense of security , architecture, bandwidth allocation etc,

Mesh mode allowed the communicating node which is a part of the network, to provide service to other nodes as describes in the figure-2. In mesh mode each node can work as a BS (service provider to the others). Mesh nodes can forward traffic to and from the multiple nodes.

The traffic flow in the mesh mode may be from the BS to SS or SS to SS or SS to BS. routing technique is also complex because a packet may be routed from the different SS'S to reach the destination. Is case of PMP packet is only routed from SS to BS or BS to SS.

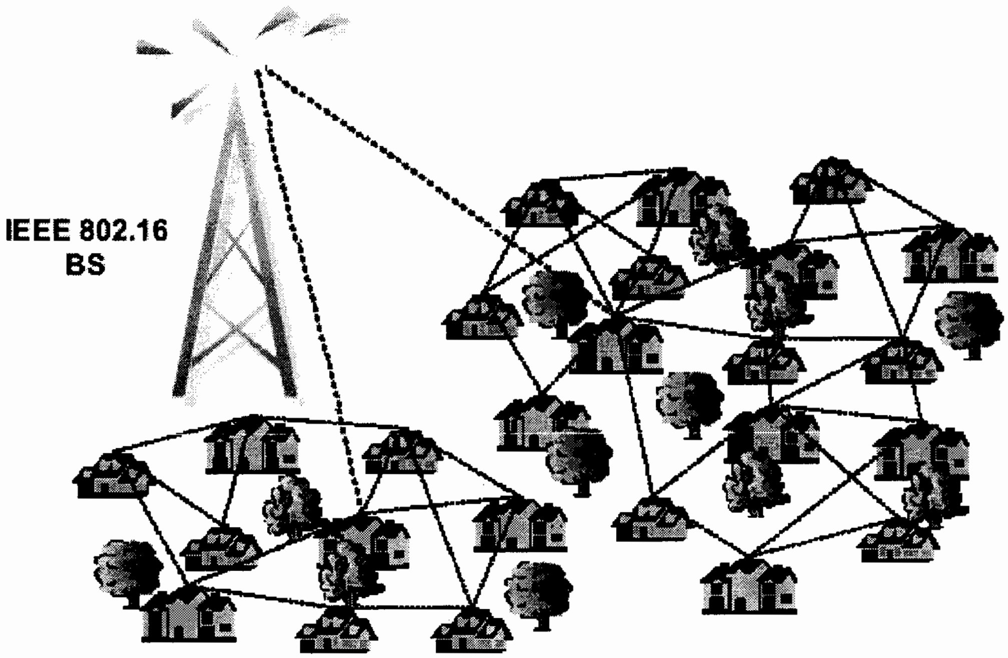

Figure 3: Mesh Mode

1.1.2 Architecture of WIMAX

The configuration in case of wireless MAN based on the 802.16 standard is some what similar to the typical cellular network. In a Point-to-Multipoint (PMP) architecture, base stations are installed in such a away as to deliver services over a radius up to several kilometers. . The sectorized antenna of base station contained in this PMP is capable of handling multiple independent sectors simultaneously. The receiver / subscriber stations (SS) generally comprise of a PCMCIA card or some inbuilt hardware that is similarly in a way like Wifi antenna in laptops. Backhaul connectivity is provided to base stations via fiber nodes or some leased lines. Client server model provides the basic road map for communication between SS and BS. BS provides the basic via media for communication through SS.

WIMAX also has the capacity to work mesh architecture. [7,10,18] it may interesting to point out , the system having direct connection to backhaul services outside mesh is called the Mesh BS while rest of the systems are termed as Mesh SSs. The Mesh BS cannot broadcast without coordinating with other nodes. Keeping in view the algorithm used, any of the scheduling technique i.e. distributing, centralized or hybrid could be harnessed See [10, 18] for details.

1.2 Motivation and Challenges

As from the establishment of the first computer network, a fast growth has been seen in the subscribers. In typical computer networks subscribers are connected to the networks via cables which have some limitations.

To establish a wired network, it requires long installation time. To cover the wide area, the longer period of time is spent. Budget for making and preservation of the wired network is also high in a huge networks. Moreover, it is difficult or not possible to wire cables across the rural areas. In this case, wired technology is not a cost-effective solution [15].

Because of these reasons, there have been many efforts to develop wireless technologies. WIMAX is the new wireless technology to meet the today's wireless needs which integrates multiple services.

1.2.1 WIMAX Security

The IEEE Standard 802.16 outlines the refuge architecture to offer privacy across the wireless network and to protect from unauthorized access.

Some parts of the security architecture are inherited from the earlier version of wireless network standard. These protocols are not intentionally designed for mesh network where trust of intermediate nodes must be taken into account. We want to investigate if there is any vulnerability related to the security architecture when the standard is deployed in mesh networks.

As compared to IEEE 802.11a/b/g based mesh network, the 802.16-based mesh networks provide higher bandwidth, range and security. The Authentication and key management protocol mentioned in [1] has some limitations in case of mesh networks. It requires some improvements for implementation in mesh mode. The author also mentioned that the protocol works only for PMP networks. He can not give any idea about WIMAX mesh. The security scheme used in [2] is implemented for PMP networks and used RADIUS as an authentication server. This technique is not useful in Mesh networks because of single authentication server (i.e. RADIUS) that increase the interference between the nodes. The level of interference depends upon how the data is routed in the WIMAX mesh network.

1.3 Background

If we consider the security aspect of the wireless technologies, they suffer from the day of evolution due to open media. Encrypted signals can also be intercepted and decrypted in easier way. Due to interception eavesdropping problems crop up, and hence, the secure transfer of the messages becomes difficult. The other major problem in wireless networks was Jamming. Someone, by sending high volume of radio signals can take down a whole network.

Many efforts have been made in order for the wireless networks to be safe. In 802.11 examples, WEP implementation was one of those, but in the end it proved to be a poor security measure. After that 802.1x was designed for a network with a fixed physical topology. Based on 802.1x, 802.11i was designed. 802.11i is the secure version of 802.11. It includes a key distribution framework that replaces the static manually configured WEP key. It also allows the use of AES encryption algorithm, But even though those enhancements to the protocol, pure implementation is a very critical factor in the security of a product and hence of the whole standard.

1.4 Research Domain

Now a days Wireless networks gained significant popularity due to their easy deployment , configuration and extension capabilities. The area of this research is WIMAX security. WIMAX security ropes two encryption standards i.e. DES3 and AES. Normally , all the traffic on 802.16 based network must be encrypted using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which uses AES for transmission security and data integrity. The security architecture of WIMAX MAC layer consists of three sub layers:

1. convergence sub layer
2. common part sub layer
3. Security sub layer.

The security sub layer provides authentication, authorization encapsulation/ de-capsulation and control management facility [17]. A new authentication and key management protocol for the mesh network is proposed.

Pakistan is the only country where WIMAX has been launched country wide by WATEEN Telecom . Number of problems has been faced in the implementation due to the following reasons.

- Interruption of licensed and unlicensed frequencies.
- Penetration
- PMP network

1.4.2 Security Architecture

Two component protocol: the first is

An encapsulation protocol for encrypting packet data across fixed network while the 2nd is A key management protocol (PKM) providing the secure distribution of keying material from BS to SS

Key Management Protocol

- A Subscriber uses the PKM protocol to get authorization and traffic keying material from the BS.
- Reauthorization and key refreshing is also done periodically through PKM.
- The keys between the BS and SS are exchanged in encrypted form through PKM which uses X.509 certificates and the RSA pubic -key encryption algorithm.
- Client/server model is followed by the PKM.
- In a client server road map , SS acts like PKM client and requests for keying material while BS PKM server responds to the requests ensuring that individual.
- Public-key encryption is used to establish a shared secret between the SS and the BS.

1.5 Proposed Approach

Readers may consider here the mesh network at two hops only. When a fresh SS/CN/TE wants to join the mesh first it scans all the available BS/NN (neighbor SS) and requests for temporary channel after the mutual authentication. New SS/CN can be first mutually authenticated by the neighboring node (NN). In this scenario when a new node is authenticated by the NN there is a no chance of malicious NN. The threat of malicious NN and CN is being removed by the mutual authentication of CN and NN by exchanging certificates and signatures. After the authentication, a channel has been provided to the CN and then CN/SS requests for the keying material to BS and subsequently uses the services of the mesh network.

In the proposed scenario when a candidate node requires the service of the network, first it scans for all the active networks. Then Candidate node sends a message to the neighboring node that contains the certificate of its manufacturer and nonce encrypted with its own private key. Trusted node (neighbor node) verifies the certificate and replies CN with own certificate and a token to avoid replay and jump forward attacks.

The mutual authentication can bypass the masquerading of both entities. After the candidate node sends a request to NN for the AK having information i.e. certificate (CN), nonce, capabilities and SAID encrypted with private key of CN. NN receives the message, un-rap it and adds its own signatures and forward it to the authentication node for the AK. Authentication node or BS receives the message and verifies the NN signature and returns the message to NN while adding four fields that are the authentication key 160 bit with 4 bit sequence number, SAIDList, Basic connection ID(BCID) and life time which gives the number of seconds before AK expires. BS sends AK while encrypting it with public key of CN and signs the whole message.

NN receives the message un-raps it, applies its own signatures and forward it to the candidate node. After receiving the AK, the candidate can use the services of the network. AK remains valid for a minimum time of 30 minutes and maximum 72 days.

After receiving the AK from the authorization node the CN requests for traffic encryption key. For this purpose it sends nonce, sequence number which represents the AK in 4 bits and SAID by applying its own signatures. Authorization node verifies the sequence number; if sequence number does not match then it gives an error message of invalid AK. If verified, replies with oldTEK and newTEK. NewTEK is encrypted with public key of CN and BS also adds nonce to avoid replay attack.This message also contains a life time field which gives the number of seconds before TEK expires. The maximum lifetime of TEK is 14 days.

1.6 Thesis Outline

This thesis is divided into three phases. In the first part, we review of the IEEE Standard 802.16 and characteristics of mesh networks is presented. The security architecture of WIMAX is also discussed with possible threats. In-depth literature review on the existing vulnerabilities found in the earlier wireless communication standard, i.e. the IEEE Standard 802.11 was also carried out. In the second phase, an analysis of the security architecture of the IEEE Standard 802.16 to identify vulnerabilities if the standard is deployed in mesh networking environments was conducted. The system design and its implementation with a possible solution are proposed to improve security for the IEEE Standard 802.16 in mesh networks. In the last portion the testing and performance evaluation are examined and also proposed the future work.

2. Literature Survey

2. Literature Survey

There are a number of research groups that are working in the area of wireless communication. These days broadband service of wireless communication is getting much popularity. Broad band facility has features that can remove the last mile problem from the Digital Subscriber Link or cable modem. There was a need of such kind of service that can solve problems relating to the expansion of wireless broad band service in the rural areas. The wireless communication is a technology that can be used as the driver which incorporates a large number of services such as Cellular, Cable TV and wireless broad band access etc. in any particular network.

In spite of the large number of advantages and features of the wireless technology, there are a number of threats that any wireless networks can face, these wireless networks are more vulnerable to security threats as compared to the wired networks. The mesh architecture in the IEEE 802.16 standard is more vulnerable to a large number of security attacks like replay attack, man in the middle attack, DoS attack etc.

Authentication, Key issuance and management is also an issue in any WiMAX network, which occur when any node join or leave the mesh network. The mesh networks use PKM version1 for authentication, key issuance and management. These security threats can damage or loss very important information in commercial operations such as E-Commerce. Since investors that are involved in such commercial business can not afford such security risks.

We studied a large number of thesis, research publications, articles, books etc, so that we can find out what has been done in this area in which our problem domain resides.

2.1 Related Research

Our literature survey has been divided into the two broad categories. These are

1. WIMAX architecture
2. Authentication and Key Management

We can not relate the authentication process of IEEE 802.16 with IEEE 802.11 because 802.11 applied shared key authentication and 802.16 uses public key authentication so both needs separate study[21].

2.1.1 WIMAX Architecture

In the first release of the IEEE 802.16 it was mentioned that WIMAX work in PMP mode only, but in the amended standard IEEE 802.16-2004 it was mentioned that this can work in mesh mode [8].

F. Akyildiz et.al. in 2005 . [22] Describe the structure of Wireless Mesh Network (WMNs). They said depending upon the architecture and deployment configuration, WMNs are mainly categorized into three main types; these are infrastructure, client and hybrids mesh.

In infrastructure mesh, mesh routers provide wireless backbone and other client connected with them. In client mesh, whole network is made up of wireless mesh clients. Client mesh has a role of routing and packet forwarding in the network. Hybrid mesh is the join of infrastructure and client mesh networks.

Asad Amir et.al. in Oct , 2006 . In [7] authors Proposed multiple wireless network interfaces on a single node, which are operating on different, non-overlapping channels in WIMAX wireless, mesh networks by making more efficient use of Radio spectrum, reducing interference and contention. They also evaluate the performance of AODV (Ad-hoc On-Demand Distance Vector) routing protocol in mesh networks.

Bongkyoung Kwon et.al , 2007. [23] Addresses the issues of malicious sponsor node, privacy and link to link encryption in WIMAX mesh by considering centralized scheduling algorithm. They say that malicious node can act as a potential node and broadcast the mesh configuration messages and lure new node to join with them. They enhanced the existing mesh authentication protocol to resolve these issues. But there solution is also expensive in computation.

2.1.2 Authentication and Key Management

David Johnston et.al. , 2004 [3]. In this paper the authors review the IEEE 802.16 standard, enumerate the security limitations like water torture attack, jamming radio spectrum , confidentiality (any one can read and write the channel), replay attack , BS masquerading can be possible, key management failure due to small two bit key and also suggest modifications to protect the standard against these threats.

But still authentication protocol is vulnerable to replay attack because they did not mention any method of key freshness and node authentication in mesh mode. If this technique is applied on mesh then there can be a threat of malicious sponsor node at the transit. The threat of replay attack is also present.

Sen Xu et.al , 2006 . In this paper the authors give overview of the IEEE 802.16 standard, focusing on MAC Layer especially on security sub layer. Enumerate the security limitations in the existing authentication and key management protocol, illustrate possible attacks and proposed some modifications in the existing authentication and key management protocol. The authors proposed the mutual authentication both for BS and SS and a secure handover roaming protocol is proposed that can be used in the future 802.16e for mobility[4].

Yun Zhou et.al In [24] authors analyze the security of IEEE 802.16 in mesh mode and find out vulnerabilities in mesh mode. Authors also suggest some improvements in WIMAX security, categorizes the attacks in five parts. In first part the authors discuss the topological attacks which includes sink hole attack (malicious sponsor node) and worm hole attack(attacker can tunnel the messages through secrete channel and reply them. Authorization attacks includes message modification between candidate and sponsor node (modification may be done by the malicious sponsor node, security level roll back attack (modification of the authentication request message which selects the weaker cryptographic algorithms and DoS (modification of the SA list which may be removal of any SA which causes even DoS). Threats to link establishment, traffic encryption keys and traffic are also discussed.

Bongkyoung Kwon et.al . [23] Describe the analysis of security mechanism based on Mesh network architecture focusing on authentication and authorization. Communication between the mesh nodes is scheduled using time division multiple access time slots. Scheduling is done by centralized algorithm, distributed algorithm or by hybrid algorithm. They give a new scheme for joining node authentication by adding two new messages in the existing scheme which is an extra burden on the bandwidth.

Fan Yang et.al . [1] Describes the analysis of security mechanism based on PMP (point-to multipoint) network architecture focusing on authentication and authorization of SS only. They give the idea of RADIUS server, in this case BS act as an intermediary between the RADIUS and the SS. They suggest some improvements in the Wireless Key

Management Infrastructure (WKMI) used for the key management through the support of Extensible Authentication Protocol (EAP).

Michel Barbeau presented in Q2SWinet '05, October 13, 2005 [5]. In this paper the author examines the threats to the security of WIMAX at physical and MAC layers. Impact and risk are evaluated and ranked by ETSI mythology.

2.1.3 Existing Protocol

There are a number of research groups that are working on IEEE 802.16 standard. The existing protocol is used for authentication of SS and also removes the replay attack on BS by mutual authentication. Chances of BS masquerading can not be ignored. The protocol for mutual authentication both for BS and SS to avoid replay attacks by including Time Stamps with each Message. The existing key management protocol is used only for PMP networks, which uses time stamp for the key freshness. In case of mesh it is difficult for second level nodes to synchronize with BS. The concept of RADIUS server was proposed which authenticates the SS; the existing key management protocol works only in PMP mode.

The existing protocol works as follows;

When any SS wants to authorize itself for network services then SS sends a message which contains the SS manufacturer's X.509 certificate. This message is optional and can be ignored. Afterwards SS sends an Authorization Request message to BS. In response to authorization request message, the BS validates the requesting SS's identity, find out the encryption algorithms and protocols to be shared with the SS, generates an AK, and sends the AK to SS. The authentication protocol is described as follows[4].

Message1.SS→BS: Cert (SS. Manufacturer)

Message2. SS→BS: [TS | Cert (SS) | Capabilities | S (2) SAID] SIG SS

Message3. BS→SS: [TS | TB | KUSS (AK) | Lifetime | SeqNo | SAIDList | Cert (BS)] SIG (3) BS

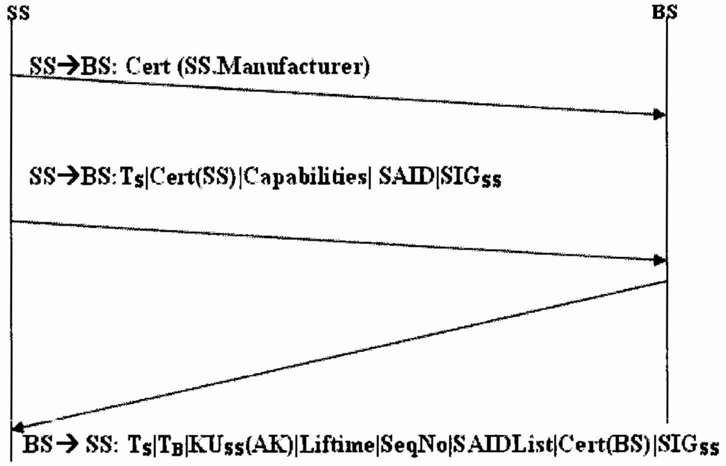
SS
BS
SS→BS: Cert (SS.Manufacturer)
SS→BS: Ts|Cert(SS)|Capabilities| SAID|SIGss
BS→ SS: Ts|TB|KUss(AK)|Lifetime|SeqNo|SAIDList|Cert(BS)|SIGss

Figure 4: Existing Authentication Process for PMP

In Message1 Cert (SS. Manufacturer) is the X.509 certificate of the manufacturer of SS. The X.509 fields consists of the certificate version, serial number, signature, issuer, validity, subject, public key info, issuer unique ID, subject unique ID, and extensions. Capabilities show SS-supported authentication and data encryption algorithms. Primary security association ID (SAID) can be equal to the BCID. AK is the authentication key that is encrypted with the public key of SS i.e. KU_{SS} (AK). A 4-bit SeqNo is used for AK. Lifetime shows the life of AK, after which AK will expires (32 bits). At the end SAIDList shows the identities and properties of the single primary SA and zero or more static SA's [4].

As Message1 is optional and can be ignored, we begin security analysis from the next message. Previous protocol has life time in Message 3 we remove it in case of mesh. After the authentication, existing protocol did not have the ability to uniquely identify the node [4].

Message1. BS→SS: [TB2 | SAID | SeqNo | HMAC (1)

Message2. SS→BS: [TB2 | TS2 | SeqNo | SAID] HMAC (2)

Message3. BS→SS: [TB2 | TS2 | SeqNo | SAID | OldTEK| NewTEK | HMAC (3)

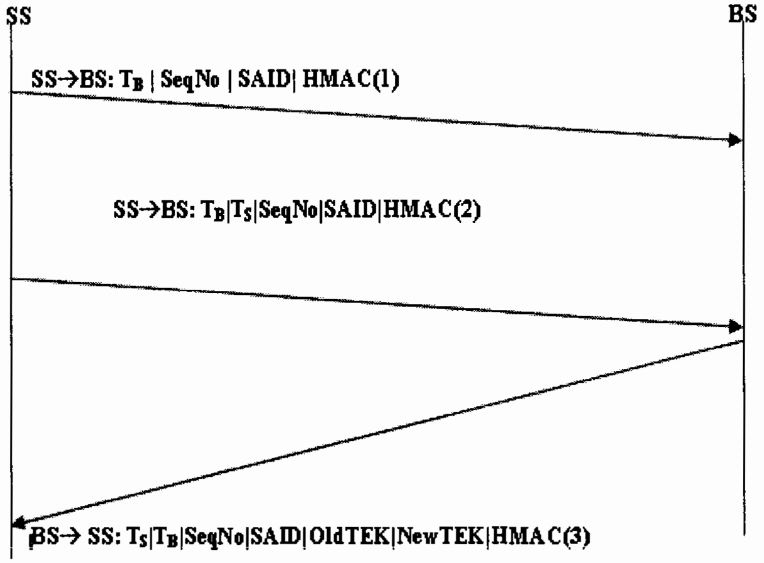
SS
BS
SS→BS: T_B | SeqNo | SAID| HMAC(1)
SS→BS: T_B|T_S|SeqNo|SAID|HMAC(2)
BS→ SS: T_S|T_B|SeqNo|SAID|OldTEK|NewTEK|HMAC(3)

Figure 5: Existing Key Management Process for PMP

The above protocol is only for the PMP networks. In case of mesh when message1 send by the SS periodically it creates lot of traffic on the network. To save the band width of the network Message1 may be omitted. Proposed key management protocol in also have a threat of repudiation in Message2 and Message3, to avoid such kind of attack SIG of SS in the Message2 and that of BS in Message3 may be included. In case of mesh Hash calculation consumes the processing capability of each node in both cases for BS and SS. When SS request for the keying information to BS, it sends the KU_{SS} to BS and BS reply by sending the NewTEK encrypted by the public key of SS.

2.2 WIMAX Applications

WIMAX is designed for broadband wireless that enables large number of vendors to manufacture huge equipment. The manufactured equipment use same standard which was mentioned in IEEE 802.16 standard. This results in lessening the cost and improves the vendor's economy. Some WIMAX applications are as follows.

1. WIMAX can connect users, enterprises and hotspots at a higher data rate.
2. WIMAX can be used to for a larger number of applications that uses VoIP services.
3. WIMAX can be used a substitute for last mile DSL or T1 level connection to businesses and homes users.
4. WIMAX can connect different networks with each other
5. Can be used for backhaul connectivity.
6. The mobility feature will allow numerous mobility based services to be offered in future.

2.3 Limitations

Currently WiMAX has not many implementations as compared to WiFi.The main reasons is unavailability of WIMAX equipment in the market. A number of manufacturers are currently working for the indoor and outdoor Customer Premises Equipment (CPE) and laptop PCMCIA cards but with limited results.

We focus on the authentication and key management issues in WIMAX. In our analysis, since the standard is new and which needed some amendments. The following limitations have been observed.

1. WIMAX is mostly suitable for backhaul, not for PMP Networks
2. Use of time stamp requires proper synchronization which is possible in PMP networks only.
3. Use of time stamp requires proper synchronization which is not possible in mesh due to intermediary nodes.

4. In case of mesh a malicious neighbor/sponsor node can participate in the network.
5. Authentication key is generated by BS only. No role of SS so SS should trust on the BS.
6. In case of PMP Session is maintained by the central node which creates lot of problem when users become enormous.
7. Same TEK is used both for uplink and downlink traffic.
8. Key Management technique works only for Point to multipoint (PMP) networks
9. An authentication and authorization needed for new node at entry level in mesh networks.
10. Key Management Technique uses HMAC which is expensive in computation and power consumption.

2.4 Goal

WIMAX predecessor WiFi (802.11 WLANs) security related problems were found out. To limit similar problems for WIMAX, it is essential to carefully assess WiMAX security model and bring improvements in the existing security architecture.

The main objective of the thesis is to analyze the WIMAX authentication and key management protocol, security architecture, encryption schemes used, try to find the limitations while implementing this protocol in mesh mode and try to remove the limitations in authentication and key management process by introducing a new authentication and key management protocol for mesh networks, to analyze the IEEE Standard 802.16 authentication and key management protocol for PMP networks, security architecture, to identify vulnerabilities, and to propose new authentication and key management protocol for the 802.16 Mesh networks. Proposed protocol mitigates the security threats like replay attack, man in the middle attack, jumping forward, water torture attack, malicious neighbor node and spoofing etc. It also reduces management messages size.

2.5 Summary

These days' wireless networks are becoming more popular due to their self configuring capability and simple use. Because of these, wireless networks are more susceptible to outside threats when compared them with wired networks. A number of security restrictions are basic problems in the expansion of these wireless networks. The existing solution available for the authentication and key management are not enough to meet the necessities of the mesh. A WiMAX mesh network requires efficient and economical solution. By designing the new system scalability also kept in mind.

In the next chapter we described the problem scenario and focus of research of the proposed system.

3. Requirement Analysis

3. Requirement Analysis

Security is a hot issue whether the networks is wired or wireless. Everyone wants that his/her data should be secured from any kind of internal or external threats. Both the System and Network Administrators are working to make networks secure. The security objectives can be broadly divided into following categorized:

1. Secrecy – keeps information confidential and any unauthorized user can not access it.
2. Authentication – Authenticity of users that want to share or access data or information.
3. Non-repudiation – Neither the sender nor the receiver can wrongly deny about sending or receiving a certain message.
4. Integrity Control – Certify that the received information is not altered or the information is in its original form.
5. Availability – Ensures availability of the system whole the time without any problem.

Network Security is applied using one or a group of the following methods:

1. Cryptography
2. Symmetric-Key Algorithms
3. Public-Key Algorithms
4. Digital Signatures
5. Authentications Protocols
6. Firewalls, VPNs, etc.

3.1 Layered architecture of IEEE 802.16 Protocol

The IEEE 802.16 Protocol stack is shown in figure 6. Physical layer (PHY) is at the bottom which deals with transmission of data. The Medium Access layer (MAC) is above the PHY layer. MAC layer consists of three sublayers[4].

- Privacy sublayer
- MAC Common Part sublayer
- Service Specific Convergence sublayer

The Privacy sublayer performs authentication, encryption, decryption, and key management. The MAC Common Part sublayer ensures the creation of MAC PDUs, channel access, connection establishment, QoS and bandwidth management. The Service Specific Convergence Sublayer coordinates with the upper layers and converts units of data of higher level protocols (e.g., IP Packets or ATM cells) to MAC Service Data Unit (SDU) format and vice versa[4].

3.1.1 Physical Layer (PHY) Details

The IEEE 802.16 physical layer allows operations that in a wide range of spectrum allocations. Physical layer operates in the following three main frequency bands.

- 10 to 66 GHz (licensed band)
- 2 to 11 GHz (licensed band)
- 2 to 11 GHz (unlicensed band)

In the LOS 10 to 66 GHz PHY specifications are required; single-carrier modulation is selected for this reason. In the PMP architecture, BS broadcasts a TDM signal.

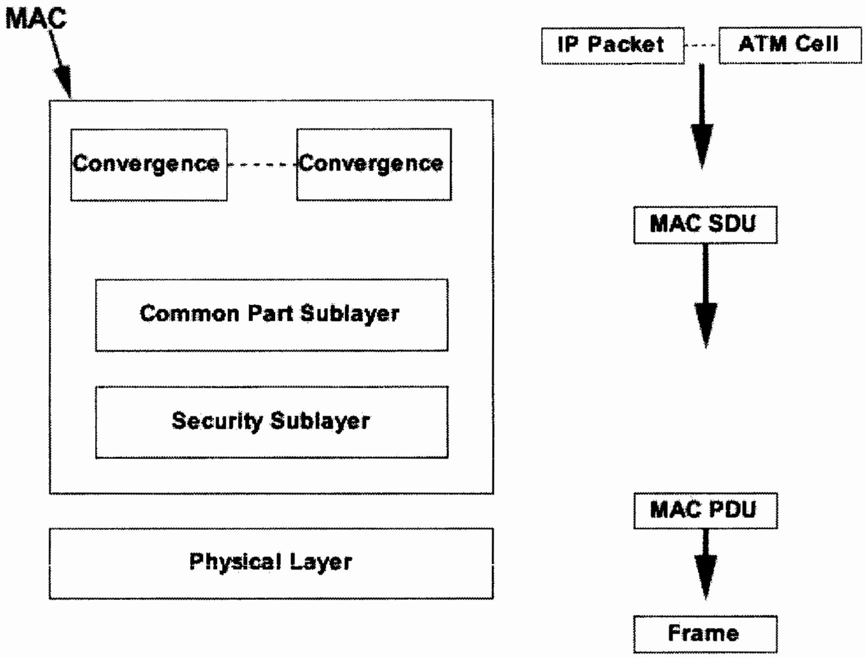

Figure 6 – Exchange of data units among layers of 802.16 [4]

NLOS can operate both in licensed and unlicensed frequencies ranging from 2 to 11 GHz bands. Three air interface specifications (given in 802.16a) supported for this band are [3]:

- WirelessMAN SC2: uses a single-carrier modulation format
- WirelessMAN-OFDM: uses OFDM with 256-point transform
- WirelessMAN-OFDMA: uses OFDMA with 2048-point transform.

3.1.2 802.16 MAC Layer (MAC) Details

- **Service Specific Convergence Sublayers**

IEEE Standard 802.16 there are two common service-specific convergences sublayers that maps services to and from 802.16 MAC connections. The ATM convergence sublayer is used for ATM services, and the packet convergence sublayer is used to map packet services like IPv4, IPv6, Ethernet, and virtual local area network (VLAN). The main objective of the sublayer is to categorize service data units (SDUs) to the appropriate MAC connection [2, 6].

- **MAC Common Part Sublayer**

In IEEE standards MAC corresponds to MAC Common Part Sublayer. In 802.16 MAC is connection oriented. In the version that supports mobility, the MAC Common Part Sublayer offers handover actions.

- **Privacy Sublayer**

The layer that deals with the security issues is the privacy sublayer. There are five components of IEEE 802.16 security architecture [3]: These are,

1. The Security Associations (SA)
2. X.509 certificates
3. PKM authorization
4. Privacy and Key Management protocol
5. Encryption

PKM uses security associations (SAs). The SA consists of a set of cryptographic methods and the related keying material; such as, it contains information which algorithms and, which key will be used. Each SS launch minimum of one SA during initialization. For the authentication and authorization key exchange the PKM protocol utilizes X.509 digital certificates along with RSA public key encryption for SS.

The architecture of Privacy layer works same in both standards i.e. fixed and mobile versions apart from the Extensible Authentication Protocol (EAP) encapsulation / de-capsulation [20].

3.1.3 Wired vs. Wireless Security

Wired networks provide many more security features than wireless networks because the security standards of wireless networks are perfectly established, easy to implement and does not depend on equipment. Because of that wired networks are less vulnerable to hackers and crackers. By using algorithms or penetration programs hackers can get unauthorized access to wireless networks or devices.

3.1.4 WIMAX Security

In IEEE 802.16 standard/ WIMAX security is employed as the MAC privacy sublayer of the protocol stack of the standard. The next section briefly describes the main component of WIMAX security.

3.1.4.1 X.509 Digital Certificates

X.509 is a standard of ITU-T for public key infrastructure (PKI). These certificates are used to identify the parties that want to communicate with each other. The X.509 certificate consists of the following fields [3]:

1. X.509 certificate format version 3.
2. Certificate serial number.
3. Certificate issuer's signature algorithm Public Key Cryptography Standard.
4. Certificate issuer.
5. Certificate validity period.
6. Certificate subject that is, shows the identity of certificate holder's
7. Subject's public key, that refers to the certificate holder's public key
8. Signature algorithm corresponds to the certificate issuer's signature algorithm.
9. Issuer's signature

The extension of the X.509 certificate not defined. Two types of 802.16-2004 standards are; manufacturer certificates and SS certificates. BS certificate is not defined. The manufacturer certificate shows the manufacturer of IEEE 802.16 device. This can be a self signed certificate or it can be issued by any third party. The SS certificate identifies any particular SS that includes SS's MAC address in the subject field. Manufacturers usually generate and sign SS certificates. The BS usually utilizes the public key of the manufacturer's certificate to validate the certificate of SS certificate, and thus recognize the device whether genuine or not [4].

3.1.4.2 Security Associations

Any security association (SA) contains security information for a BS and one or more SSs that wants secure communication. This security information consists of the cryptographic suite engaged within the SA [3]. There are three types of SAs. These are:

- *Primary SAs* – created during SS initialization process
- *Static SAs* – This is provisioned by BS. Also Can be shared by several SSs
- *Dynamic SAs* – created and removed when not used, multiple SSs can share it

As IEEE 802.16 standard uses two SA types; i.e. *data a*nd *authentication SA* .The data SA consists of the following [3]:

- A 16-bit SA identifier, or SAID.
- A cipher that is used for secure data exchanged. (802.16-2004 make use of DES in cipher block chaining (CBC) mode; this design can be used for other algorithms.
- Two traffic encryption keys (TEKs) that are used to encrypt data: i.e. the present TEK in use and another TEK when existing TEK in use will expires.
- Two 2-bit key identifiers for both keys.
- A TEK lifetime. The default value is half a day and a minimum value of 30 minutes and a maximum value is seven days.
- An initialization vector of 64-bit for each TEK.
- Type of data SA. (Primary, static or dynamic).

The authorization SA consists of the following [3]:

- X.509 certificate that identify the SS.
- Authorization key (AK) of 160-bits.AK is used that show authorization to get access of IEEE 802.16 transport connections.
- A 4-bit SeqNo that is used to identify the AK.
- AK lifetime can be from one to 70 days. Default lifetime value is seven days.

- Key encryption key KEK that is used to distribute to TEKs. The KEK is created as: KEK = Truncate-128(SHA1 (((AK | 0^{44}) XOR 53^{64})), where Truncate-128(.) is used to the first 128 bits, *a* | *b* indicates the concatenation of strings *a* and *b*, a^n indicates the octet *a* will repeats exactly *n* times, and SHA1 is used for secure hash calculation.
- Downlink hash function message authentication code (HMAC) is used to provide authenticity when the key is distributed from BS to SS. The key is defined as: Downlink HMAC key = SHA1((AK | 0^{44}) XOR A^{64}).
- Uplink HMAC key provides data authenticity when the key is distributed from SS to BS. The uplink HMAC key is defined as: Uplink HMAC key = SHA1((AK | 0^{44}) XOR $5C^{64}$).
- A list of all the authorized data SAs.

3.1.4.3 Cryptographic Suite

A cryptographic suite defines a set of SA's methods used for data encryption, TEK exchange and data authentication.

3.1.5 Privacy and Key Management Protocol

A PKM protocol creates a data SA between BS and SS. Two or three-messages are exchanged between SS and BS. BS utilizes first message, which is an optional message, used for re-keying of a data SA or used to construct a new SA. If not, SS starts protocol after sending the second message, and finally BS replies with the third message [3].

Message 1: BS →SS: SeqNo | SAID | HMAC(1)
Message 2: SS →BS: SeqNo | SAID | HMAC(2)
Message 3: BS →SS: SeqNo | SAID | oldTEK | NewTEK | HMAC(3)

The SeqNo shows the sequence number of the AK in use. The HMAC(1) shows the HMAC SHA-1 digest of the SeqNo | SAID by using AK's downlink HMAC key, its value can be used by SS to detect forgeries. SS sends Message 2 for requesting SA's parameters. SS uses SAID, which is available in the authorization protocol SAIDList or from a Message 1. SS creates another Message 2 for each data SA.HMAC (2) is the HMAC SHA-1 digest of SeqNo | SAID when AK's uplink HMAC key is used. BS will authenticates SS by HMAC(2) since: only SS has the ability to unwrap the AK, which was sent in Message 3. Now if HMAC(2) is valid and SAID show one of SS's SAs, BS configures SA by using Message 3. The OldTEK value repeats the active SA parameters and the NewTEK value which is used when the current TEK expires.

The fixed version of 802.16 uses one way RSA authentication based on PKMv1 from SS to BS. The security mechanism for 802.16e differs because it uses mutual authentication. The RSA authentication protocol that supports mobility is given below [20]:

Message 1: SS →BS: Cert (Manufacturer (SS))
Message 2: SS →BS: ns, Cert (SS), SAID, Sig(SS)
Message 3: BS →SS: ns, nb, $\{\text{prePAK}\}_{\text{Pk(SS)}}$, PAKNr, Cert(BS), Sig(BS)
Message 4: SS →BS: nb, Sig(SS)

In Message 1 SS sends its manufacturer's certificate to BS. This message is optional. After this message, SS sends a nonce (random value), its own certificate and SAID to requests for keying material. This message is signed by SS. In response, BS sends a message having SS nonce, its own nonce (nb), the pre Primary Authentication key (prePAK) encrypted with public key of SS, sequence number of prePAK (PAKNr), its own certificate and signatures.At the end SS acknowledges receiving the BS message by sending BS nonce (nb) signed by SS [20].

3.1.6 Encryption Schemes

IEEE 802.16 standard uses the Privacy and Key Management (PKM) protocol for the authentication of SS to BS and for exchange of keying material.

For data encryption, the Data Encryption Standard (DES) with the cipher block chaining (CBC) mode with 56-bit keys. Advanced Encryption Standard (AES) can also be used in Counter mode with CBC-MAC .The encryption keys are transferred between SS and BS using 3DES with a key exchange key derived from the authorization key.

Finally, message authentication in very important MAC functions, like connection setup, will provide by the PKM protocol. The PKM protocol messages are authenticated by using the Hashed Message Authentication Code (HMAC) protocol with SHA-1[3,20].

3.2 Problem Scenario

When considering WiMAX mesh networks little work is previously done. In WIMAX PMP networks all data is routed through BS i.e. from BS or to BS. In mesh SS be connected to BS through other SS. Existing authentication protocol for mesh requires some improvements because there are a number of possible threats like Replay Attack, DoS Attack, Jump forward Attack and BS/SS masquerading etc. may exist during their implementation. In the proposed scenario three communicating nodes are involved. These are BS, NN and SS. NN is a neighboring/sponsoring node which authenticates the new node that wants to enter in the mesh network. Mutual authentication of both SS and NN is performed at the first step. All types of attacks will be mitigated after using the proposed protocol. The performance of BS will also improve when our proposed protocol will be used.

3.3 Focus of Research

Our research focus will be on WIMAX mesh network security issues which involve authentication/authorization and key management. Through literature survey first we analyze the existing authentication and key management protocol in WIMAX networks. Mentioned some limitations while implementing this protocol in mesh mode of WIMAX. Previous protocols are vulnerable to threats like malicious neighbor ,replay attack and spoofing. In the proposed authentication/authorization and key management protocol these threats are mitigated in Mesh mode.

3.4 Summary

In this chapter all the requirements for the implementation of security were discussed. Since there are many components that are involved for security. These include secrecy, authentication, non-repudiation, integrity control and availability. The architecture of IEEE 802.16 was also discussed in detail. Digital signatures were also discussed that are used to sign the message during communication for secure and authenticated communication. Finally, cryptographic suit also described.

In the next chapter we discuss the system design in detail.

4. System Design

4. System Design

During the design phase all the aspects of the project are going to be covered, which is further used for the coding and the implementation can be directly completed.

In the first phase of this thesis we gather requirement analysis of the proposed research topic i.e. about the authentication and key management protocol. Review the literature related to IEEE Standard 802.16 and characteristics of mesh networks including vulnerabilities in mesh.

In second phase analyses the existing authentication and key management protocol for WIMAX PMP network and identify some vulnerability if that is deployed in mesh networking environment. We also review the authentication technique used in 802.11 mesh.

In last phase, possible solution is proposed for mesh networks.

4.1 Research Method

During the design stage all the feature of the protocol are included and coding, implementation in performed on these procedures. The research is performed by using the conductive method. Understanding and profound study of the problem was presented by involving qualitative methods. Throughout the research, literature reading was completed, through Internet and IEEE's website, where most recent reports about the protocol was available.

4.2 Reference Architecture

The mesh architecture has been considered for the proposed system. In the proposed scenario base station (BS), neighbor node (NN) and candidate node (CN) which is a new node that enters the mesh network. Authentication is performed when any node join the mesh network, when authentication succeeds, the new node request for Traffic/Transport Encryption key. TEK is used for encrypting the data messages between SS and BS. When a candidate node joins the network the following messages are exchanged for the authentication.

AuthRequest: CN→NN: Ccrt (CN)

AuthReply: NN→CN: Cert (NN) |TKN|SIG_{NN}

AKRequest: CN→NN: Nonce $_{CN}$ |TKN|Capabilities|SAID|SIG_{CN}

AKRequest: NN→BS: Nonce $_{CN}$ |Cert (CN) |Capbilities|SAID|SIG$_{NN}$

AKReply: Nonce$_{CN}$|Nonce$_{BS}$|KU$_{CN}$ (AK) |SeqNo|SAIDList|Cert$_{BS}$ (Manf.)|SIG$_{BS}$

AKReply: Nonce$_{CN}$ | Nonce$_{BS}$ | KU$_{CN}$ (AK)|SeqNo|SAIDList| Cert$_{BS}$ (Manf.)| SIG$_{NN}$

The description is each message exchanged is as follows:

AuthRequest: CN→NN: Cert (CN)

AuthRequest: Message CN requests NN for mutual authentication. CN sends NN its certificate containing signatures and public key. NN maintain an authentication level, which is a table having fields one for MAC address and other for a numeric value, which will be either 0 or 1. When first request comes from a CN at that time NN make the authentication level one against her MAC address. Now if again any request comes from that MAC during the processing of the first request NN checks its authentication level if it is 1 then she ignore the request and discard it. If its authentication level is 0 then it processes its request. Authentication level is used to control replay attacks in effective manner as compared to time stamp or nonce.

AuthReply: NN→CN: Cert (NN) |TKN|SIG$_{NN}$

After processing the Authrequest NN generates a token makes its entry in the authentication level table and issue it to requesting CN. If both CN and NN mutually authenticate each other then CN can now requests for authentication key.

AKRequest: CN→NN: Nonce $_{CN}$ |TKN|Capabilities|SAID|SIG$_{CN}$

Now when CN request for the AK she also attach that token. After receiving the request from the CN , before forwarding it to the base station , NN first checks the token (which shows it is a mutually authenticated node) if it does not match with the entry in authentication table then NN reply with an error message if it matches then NN forward the request to BS/Authentication Server for the issuance of AK and also make the authentication level 0 against that MAC.

In the AKRequest message CN sends NN its credentials, which includes CN's nonce, token (TKN), capabilities list, SAID. All the information which CN sends is signed with SIG$_{CN}$. Now NN receives the AKRequest message,verify the TKN and forward request to BS with its own signatures. NN includes CN's Certificate instead of TKN in the message.The purpose of token is to avoid jumping forward and replay attacks.

AKReply: Nonce$_{CN}$|Nonce$_{BS}$|KU$_{CN}$ (AK) |SeqNo|SAIDList|Cert$_{BS}$ (Manf.)|SIG$_{BS}$

In response of AKRequest message BS/Authentication server generate AK, encrypt it with the public key of CN, adds its own certificate and signatures for the authenticity and send it to the NN for forwarding it to CN. Authentication server also keeps the record of AK (160 bit) against her MAC and SeqNo (4 bit) in a temp table.

BS receives the AKRequest, sends AK and SeqNo. encrypted with CN's public key to the NN. NN again forward this AKRelpy to CN.

Finally CN receives the AKRequest response. Decrypt it and use AK to obtain TEK (Traffic Encryption Key) from BS.

After successful authentication the node new requests for Traffic Encryption key (TEK). These two messages are exchanged for TEK requests.

Message1. SS→BS: Nounce$_{SS}$ | SeqNo | SAID] SIG$_{SS}$

Message2. BS→SS: Nounce$_{BS}$ | Nounce$_{SS}$ | SeqNo | SAID |oldTEK| KU$_{SS}$(NewTEK) |SIG$_{BS}$

4.3 Methodology / Algorithm

We consider each system in mesh network which is called a node. Other nodes which directly connect to a node(BS) are neighbors at level 1(N1) , and all nodes connected to neighbors(N1) of the neighborhood called neighbor at level 2 (N2) – in other words, nodes one-hop away from the node are N1 neighbors, and nodes two-hop away from the node are N2 neighbors. The node, its neighbors N1, and neighbors N2 are shown in Figure 7.

The Mesh BS is used for connecting to outside backhaul services and other nodes are describes Mesh SSs. Like to the PMP mode, downlink is referred as transmission from the Mesh BS, and uplink is referred as transmission to the Mesh BS.

Proposed protocol for the authentication in mesh mode is illustrated as

AuthRequest: CN→NN: Cert (CN)

AuthReply: NN→CN: Cert (NN) |TKN|SIG$_{NN}$

AKRequest: CN→NN: Nonce $_{CN}$ |TKN|Capabilities|SAID|SIG$_{CN}$

AKRequest: NN→BS: Nonce $_{CN}$ |Cert (CN) |Capbilities|SAID|SIG$_{NN}$

AKReply: Nonce$_{CN}$|Nonce$_{BS}$|KU$_{CN}$ (AK) |SeqNo|SAIDList|Cert$_{BS}$ (Manf.)|SIG$_{BS}$

AKReply: Nonce$_{CN}$ | Nonce$_{BS}$ | KU$_{CN}$ (AK)|SeqNo|SAIDList| Cert$_{BS}$ (Manf.)| SIG$_{NN}$

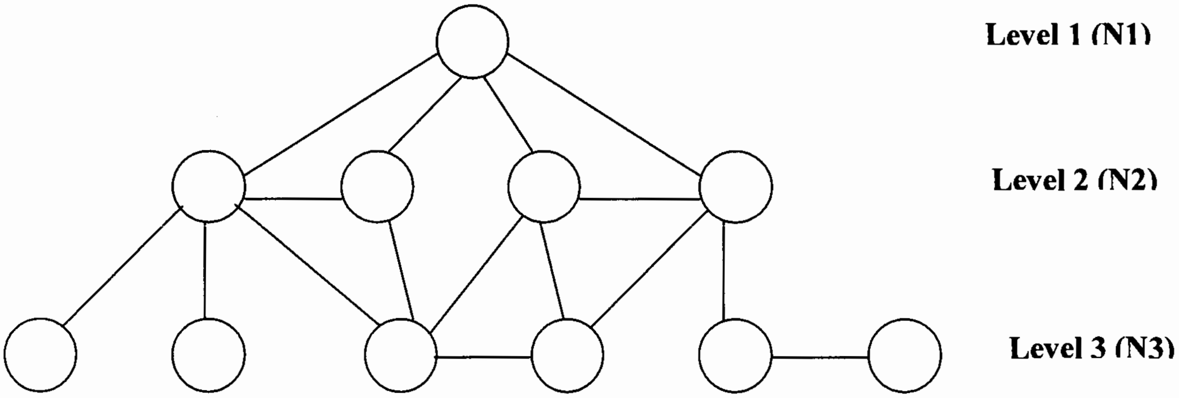

Figure 7: Neighbor at level 1(N1), at level 2 (N2) nodes and at level 3(N3)

In the proposed system when any candidate node wants to use the service of the network, initially it scans for all the active networks. CN requests for mutual authentication and sends an AuthRequest Message. CN sends NN its certificate and signatures in AuthRequest. NN maintain an authentication level, which is a table having fields one for MAC address and other for a numeric value, which will be either 0 or 1.Authentication level is used to control replay attacks. In response of AuthRequest message if CN's certificate will be valid then NN sends a token to CN along with its own certificate and signatures. The Token is used to avoid from jump forwarding. If both CN and NN mutually authenticate each other then CN can now requests for authentication key.

In the AKRequest message CN sends NN its credentials, which includes CN's nonce, token (TKN), capabilities list, SAID. All the information which CN sends is signed with SIG$_{CN}$. Now NN receives the AKRequest message,verify the TKN and forward request to BS with its own signatures. NN includes CN's Certificate instead of TKN in the message. BS receives the AKRequest, sends AK and SeqNo. encrypted with CN's public key to the NN. NN again forward this AKRelpy to CN.

Finally CN receives the AKRequest response. Decrypt it and use AK to acquire TEK (Traffic Encryption Key) from BS.

After receiving the AK, now candidate can use the services of the network. AK will be legal for a minimum time of 30 minutes and maximum of 72 days

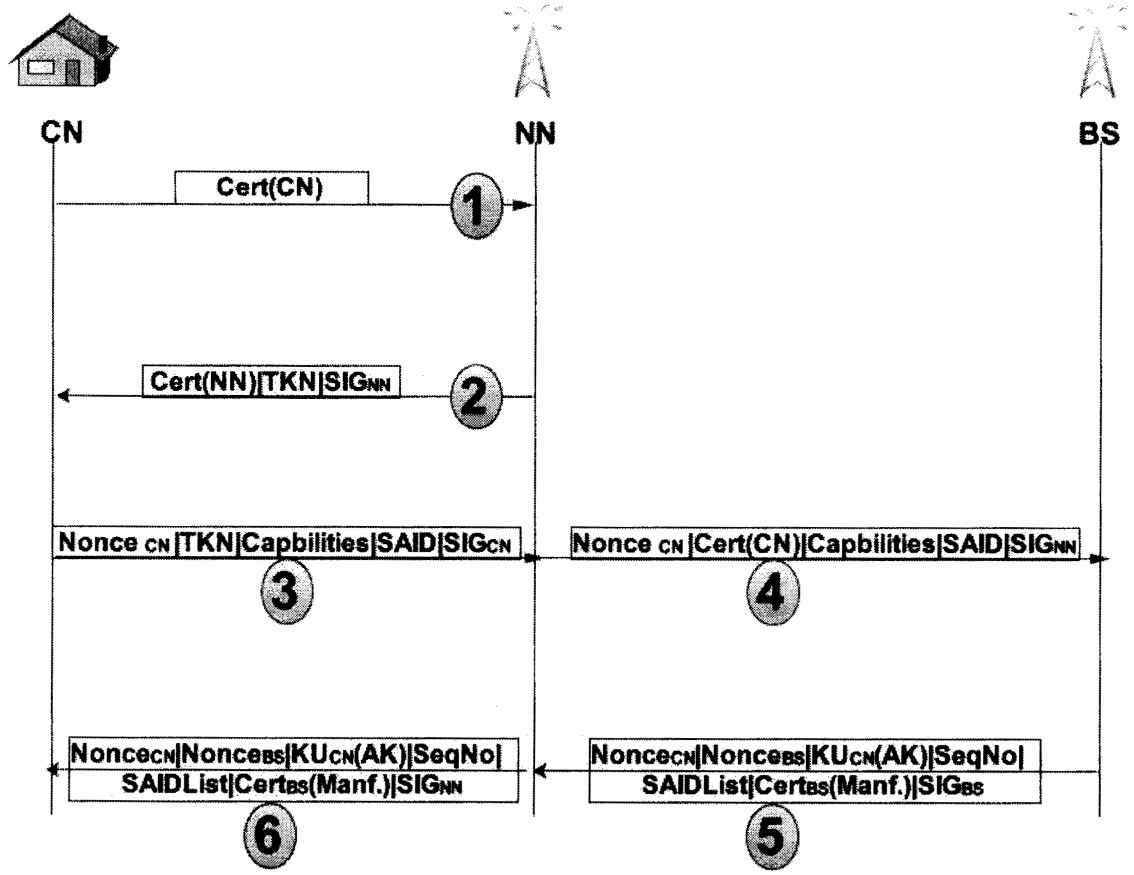
CN
NN
BS
Cert(CN)
1
Cert(NN)|TKN|SIGNN
2
Nonce CN |TKN|Capbilities|SAID|SIGCN
3
Nonce CN |Cert(CN)|Capbilities|SAID|SIGNN
4
NonceCN|NonceBS|KUCN(AK)|SeqNo| SAIDList|CertBS(Manf.)|SIGNN
6
NonceCN|NonceBS|KUCN(AK)|SeqNo| SAIDList|CertBS(Manf.)|SIGBS
5

Figure 8: Authentication Process

M1. SS→BS: [Nonce $_{S}$ | SeqNo | SAID] SIG$_{SS}$

M2. BS→SS: [Nonce $_{B}$ | Nonce $_{S}$ | SeqNo | SAID | OldTEK| KU$_{SS}$(NewTEK) | Lifetime|SIG$_{BS}$

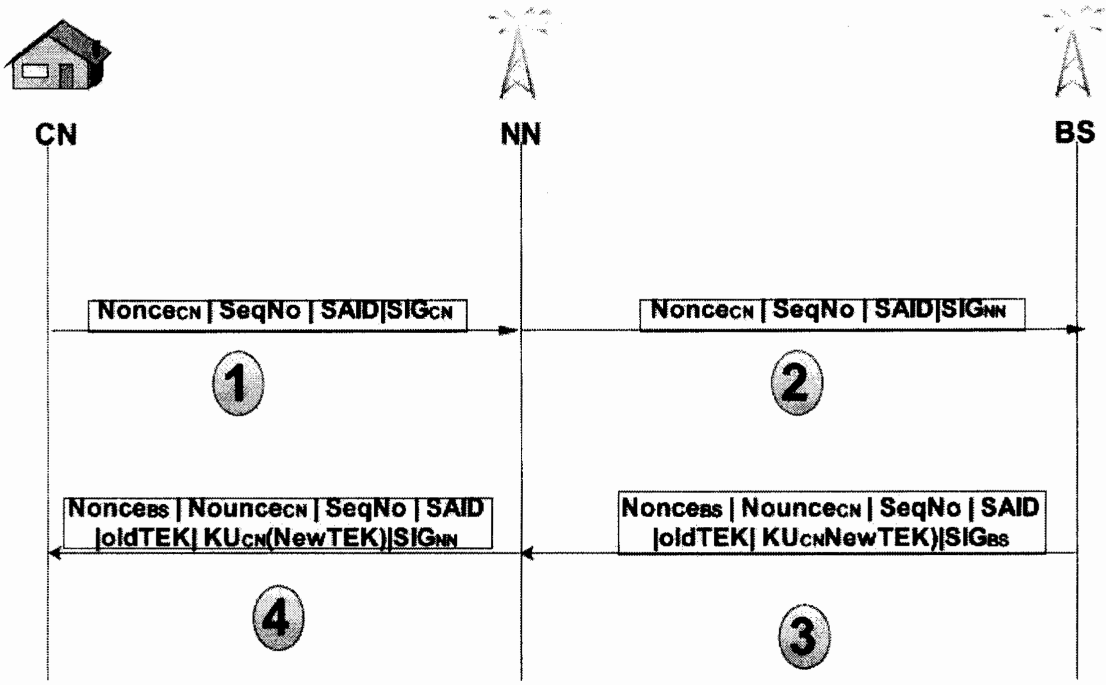
CN
NN
BS
Nonce$_{CN}$ | SeqNo | SAID|SIG$_{CN}$
1
Nonce$_{CN}$ | SeqNo | SAID|SIG$_{NN}$
2
Nonce$_{BS}$ | Nounce$_{CN}$ | SeqNo | SAID |oldTEK| KU$_{CN}$(NewTEK)|SIG$_{NN}$
4
Nonce$_{BS}$ | Nounce$_{CN}$ | SeqNo | SAID |oldTEK| KU$_{CN}$NewTEK)|SIG$_{BS}$
3

Figure 9: Key Management

After receiving the AK from the authorization node now CN request for traffic encryption key. For this purpose it send nonce, sequence number which represents the AK in 4 bits and SAID by applying its own signatures. Authorization node verifies the sequence number; if sequence number does not match then it give an error message of invalid AK. If verified, reply candidate node with oldTEK and newTEK. newTEK is encrypted with public key of CN and BS also adds nonce to avoid replay attack. This message also contains a life time field which gives the number of seconds before TEK expires. The maximum lifetime of TEK is 14 days.

Using this technique secure communication can be possible, no malicious NN can participate in the mesh network, BS bandwidth is used in more affection manner and Peer-to-peer communication can be possible.

When a node enters into a Mesh network, it shall follow the node initialization and network entry procedures. The node also follows these procedures in case of signal lost. The overview of the procedures is as follows.

1. **Scan for active networks:** The new node that wants to join the network, first scans for all active mesh networks by probing message a broadcasted from other nodes.

2. Authentication/Authorization: The new node requests the neighboring node for authentication by sending a message. SS/candidate then again sends its certificate, capabilities, SAID list, nonce, public key and signature to its neighbor who forward it to authorization node. In reply to second message the authorizing node adds BCID (to uniquely identify a node), signatures, nonce, its own certificate and authentication key encrypted with public key of SS and send it to candidate node through neighbor node. Now SS can be part of the mesh network.

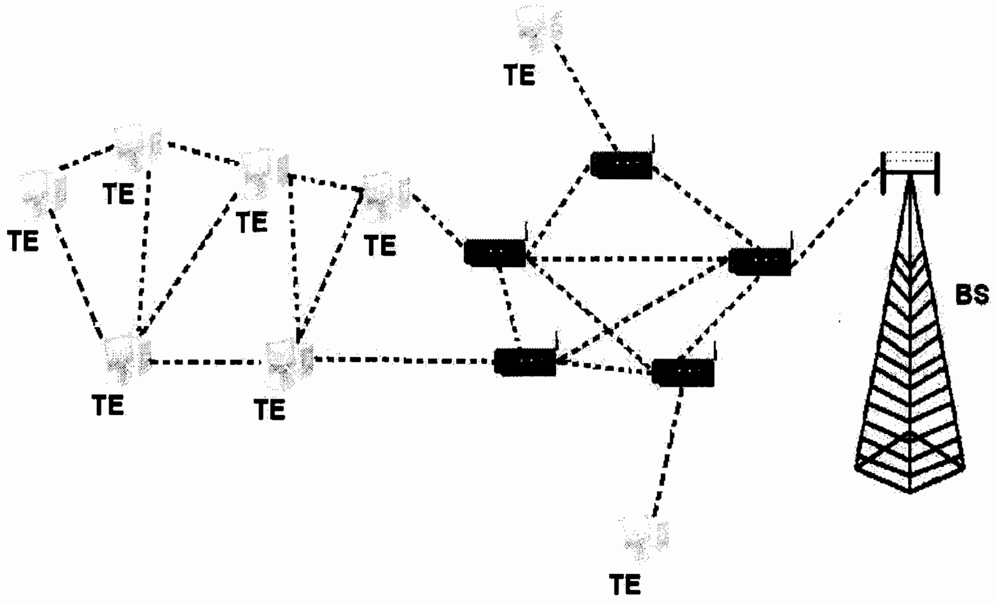

Figure 10: Architecture of Mesh Network

3. Issuance of Keys: After entering into mesh network, a candidate node desires for session and TEK keys to BS. For this reason candidate node sends its sequence number which represents the authentication key, public key, authentication key, certificate (authenticator)/MAC to BS through neighbor nod. After authentication of the sequence number, BS sends TEK Keys encrypted with public key, session to candidate node. Now node is allowed to utilize the services of the network for particular session. When the TEK of candidate node is about to expire then step three will be repeated again.

The algorithm of the proposed design is as below.

BS (Base station always in Listen mode)

```
{
{
1. Receive request from the NN(for the authentication)
2. Accept this request.
3. Reply it by sending the AK , BCID(IP) and Seq no to the NN.

}

    1. receive the request for TEK
    2. accept the request
    3. reply it with old and new TEK encrypted with CN public key

    }
```

NN (intermediate node in listen mode)

```
{
{
1. Receive request form the CN
2. Check the authentication level
   If (value=1) {
   Discard the request
}
    3. Accept the request.
    4. Generate the Token; make its entry in the authentication level table against the
       MAC Address.
    5. Reply to candidate with its own certificate, token after signing them
    6. Now CN requests for authentication key by sending token, nonce and its own
       credentials after signing them to NN.
```

```
        7. NN receive and verify the token and forward the request to BS for AK.
        8. BS generates the AK, encrypted with the public key of CN along with sequence no, signing them and send to CN through NN.
        9. After receiving the AK, now CN requests for TEK by sending nonce, SeqNo after signing them.
        10. BS verify the SeqNo and generates TEK, encrypted with RSA by using AK as a key.
    }
    11. Connected
}
```

CN (node that was requesting for the authentication)

```
{
{
1. Send request to neighbor for mutual authentication by sending its certificate.
2. Receive reply from the neighbor with information (TKN, Cert(NN), SIG NN)
}
3. Request accepted by the neighbor node for providing the temporary channel.
4. Send request to the BS through neighbor having (nonce CN, Certi CN,TKN, etc, SIG CN)
5. Neighbor receive this message and forward it to the BS (authorizing node) by Adding its own signatures now the message becomes (previous at step 4, SIG NN (NN remove the signature of CN and add its own))
6. NN receive reply from the BS including (message at step 5, nonce BS, SIG BS , SEQ no, Pre-AK encrypted with CN Public key).
7. NN forwards this message to the CN by adding its own SIG with message at step 6.
8. CN authenticated and can use the services of the network. But before using the service CN must take traffic encryption key from the BS.
9. CN sends the request for traffic encryption key (Information encrypted with private key)
10. NN forwards this request to  BS by adding its own signature.
```

11. BS reply with TEK encrypted with public key of CN to NN

12 NN forward this information to CN.

13 now CN can fully participate in mesh.

}

4.4 Summary

The most important issues which were considered in the design of the authentication and key management protocol include maliciousness of neighbor node and costly computation in several cases. Proposed protocol develops a system, which is more reliable and able to tender services to the nodes in more efficient way. Our proposed system keep both SS and BS save from the replay attack. Using the proposed protocol only the trusted parties can participate in the communication. We divide our design in three modules first the mutual authentication of the candidate and the neighbor and other in the issuance of keys from the BS and finally key management technique.

5. Implementation

5. Implementation

The coding phase of the project will include the algorithm, description of classes its implementation in Java. We choose java due to its platform independency. We also mention the functionality and requirements.

The pseudo code of the classes is going to be shown at abstract level of all the method of the classes. Furthermore the functional description of the data flow diagram of the protocol will be included. This will show the input, output and description of all the functions in the system flow diagram.

5.1 Deployment Environment

The system development, implementation and testing is the last phase of the development of the system. In this phase the new application programs are created and tested.

5.1.1 Tool/Language Selection

The choice of software is very important factor to be considered during the development phase of a new system. This decision depends upon many factors including the requirement of the system, current environment (i.e. existing software), amount of data to handle and the cost of programming. After deeply studying the nature of the problem and considering the need, we choose the Java due to its complete security solution in our system.

The developed system will be platform independent. Therefore, it can be used in any operating environment. For java programming we used JBuilder Enterprise 7.0 edition and Notepad++.EDrawer Network Diagrammer 3.0 is also used to draw diagrams.

5.1.2 Features of Java

Following are the basic features that make Java a powerful and popular programming language:

1. Platform Independence
2. Object Oriented

3. Compiler/Interpreter Combo
4. Robust
5. Several dangerous features of C & C++ eliminated:
6. Automatic Memory Management
7. Security
8. Dynamic Binding
9. Good Performance
10. Threading
11. Built-in Networking

5.1.3 OPERATING SYSTEM

The developed system can be used in any operating environment for example windows and Linux.

Hardware requirements

The following are hardware requirements:

- Any Intel based computer especially, P-III with a minimum of 128 MB RAM.
- Any type of monitor (monochrome or colored).
- Hard disk having capacity of 20 GB or greater.
- Network Interface Cards
- Connectors
- Cables

5.2 System Flow Diagram:

We divide our flow charts in the following categories

1. candidate node to neighbor node communication, mutual authentication
2. neighbor node to Base Station/authorization node communication
3. candidate node to Base Station/authorization node communication

5.2.1 Mutual Authentication of Candidate and neighbor node

Following are the protocol commands used in the mutual authentication:

AuthRequest(Authentication Request)

After scanning the network a node that needs services initiate the request of authentication to the nearly neighbor with the protocol code **AuthRequest.**

ER01(Request Time out)

When a neighbor receives a fresh request from the candidate and if the time out occurs then neighbor reply with the protocol code **ER01**.

ER02(Already requested)

After receiving the authentication request from the candidate, neighbor checks its authentication level if this is 1,request is already is in the process then neighbor discard the request and reply with a code **ER02 .**

ER03(Invalid certificate of CN)

After receiving the authentication request from the candidate, neighbor checks its certificate if it is invalid then reply with a code **ER03.**

ER04(Invalid TKN)

After receiving the authentication request from the candidate, neighbor checks its Token if this TKN did not verified then reply with a code **ER04.**

AuthReply(Authentication reply)

When a neighbor receives a fresh request from the candidate node after the verification of its certificate (certificate from the known manufacturers are considered to be trusted) and reply it with **AuthReply** code.

ER04(Invalid certificate of NN)

Upon receiving the reply from the neighbor candidate also checks the certificate of the neighbor if this invalid then reply to neighbor with code **ER04** and search for another neighbor for communication.

5.2.2 Request for the Authentication Key

AKRequest(Authentication key Request)

After the mutual authentication now candidate request for the authentication key with code **AKRequest** forwarded through neighbor which also checks whether it comes from a authenticated node or not.

ER05(NN disconnected from BS)

When neighbor receives request of authentication key from candidate and signal loss occurs then it reply with a code **ER05**.

AKReply(Authentication key reply)

After receiving the authentication request BS/Authorization node generate an AK along with SeqNo, encrypt it with the public key of candidate node and reply with code **AKReply.**

5.2.3 Request for the Traffic Encryption Key

TEKRequest(Traffic Encryption Key request)

Upon receiving AK and SeqNo now candidate request for the traffic encryption key with code **TEKRequest.**

ER06(Invalid sequence no)

Authorization node check the SeqNo before sending the traffic encryption key if it is invalid then reply with code **ER06**.

ER07(Time out (AK Expires))

Authorization node check the life time of the AK if it expires then reply with code **ER07**.

TEKReply(Traffic Encryption reply)

After the verification of the SeqNo and AK life time authorization node issue the TEK and reply with code **TEKReply** .

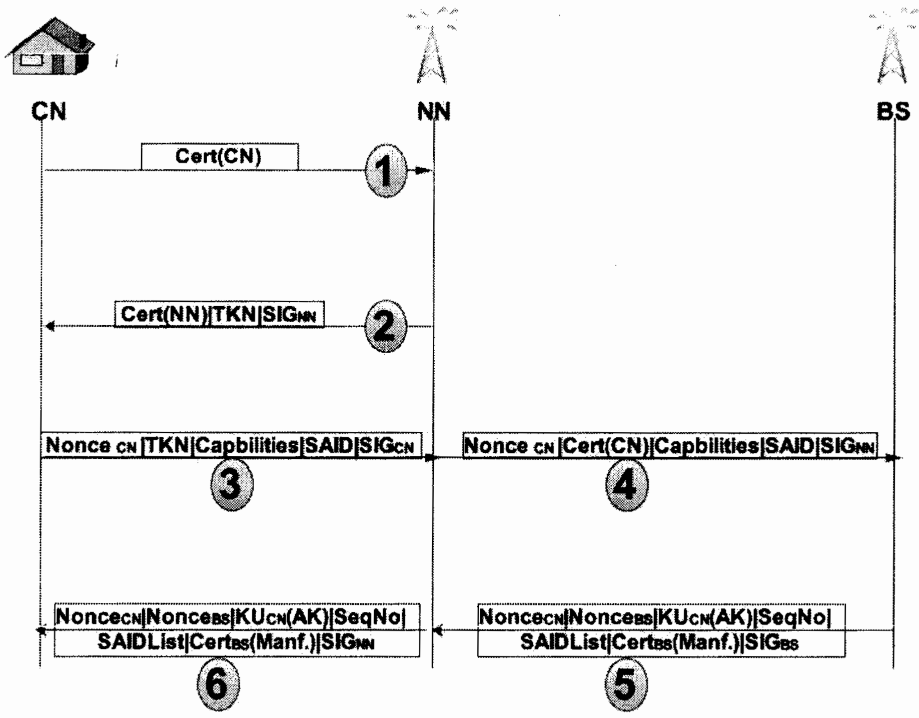
CN
NN
BS
Cert(CN)
1
Cert(NN)|TKN|SIGNN
2
Nonce CN |TKN|Capbilities|SAID|SIGCN
3
Nonce CN |Cert(CN)|Capbilities|SAID|SIGNN
4
NonceCN|NonceBS|KUCN(AK)|SeqNo|
SAIDList|CertBS(Manf.)|SIGBS
5
NonceCN|NonceBS|KUCN(AK)|SeqNo|
SAIDList|CertBS(Manf.)|SIGNN
6

Figure 11: Flow Diagram

Case-1 ER01(Request Time out)

CN → NN : AuthRequest

NN→CN : ER01 (Time out)

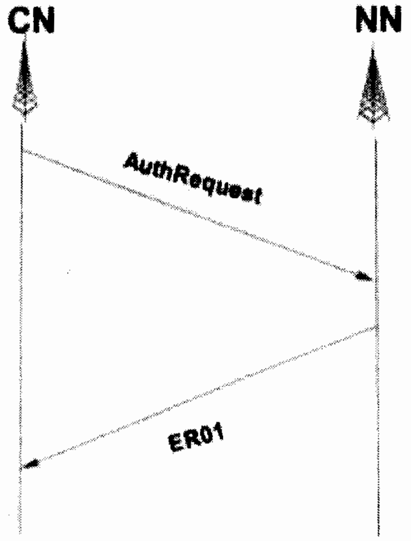

Figure 12: Request Time out in Authentication Request

Case-2 ER02 (Already Requested)

CN → NN : AuthRequest

NN→CN : ER02 (Already Requested)

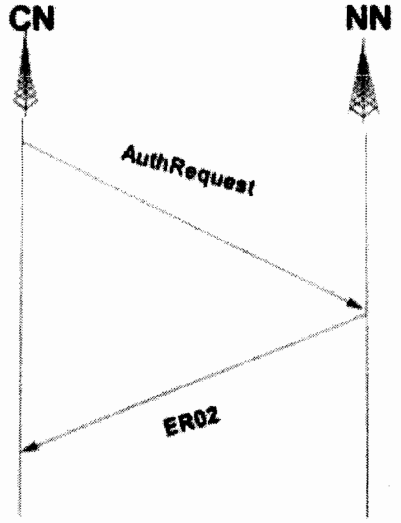

Figure 13: Already Requested in Authentication Request

Case-3 ER03 (Invalid Certificate)

CN → NN : AuthRequest

NN→CN : ER03 (Invalid Certificate)

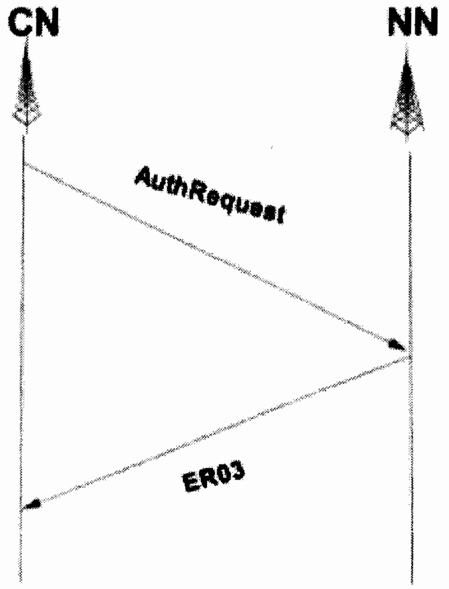

Figure 14: Invalid Certificate in Authentication Request

Case-4 ER04 (Invalid TKN)

CN → NN : AuthRequest

NN→CN : AuthReply

CN→NN: ER04 (Invalid TKN)

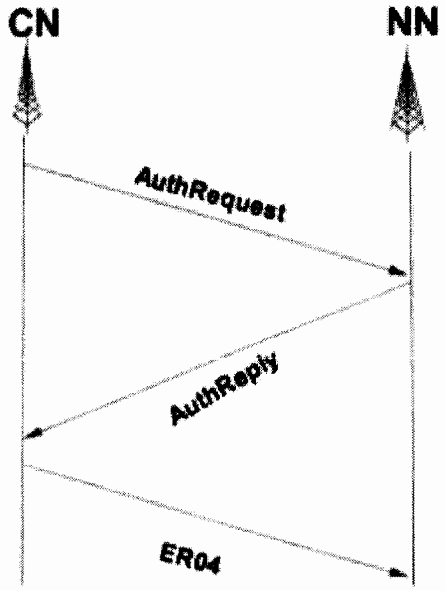

Figure 15: NN Invalid Certificate in Authentication Request

Case-5 ER05 (Disconnect from BS)

CN → NN : AuthRequest

NN→CN : AuthReply

CN→NN: AKRequest

NN→ CN : ER05 (Disconnect from BS)

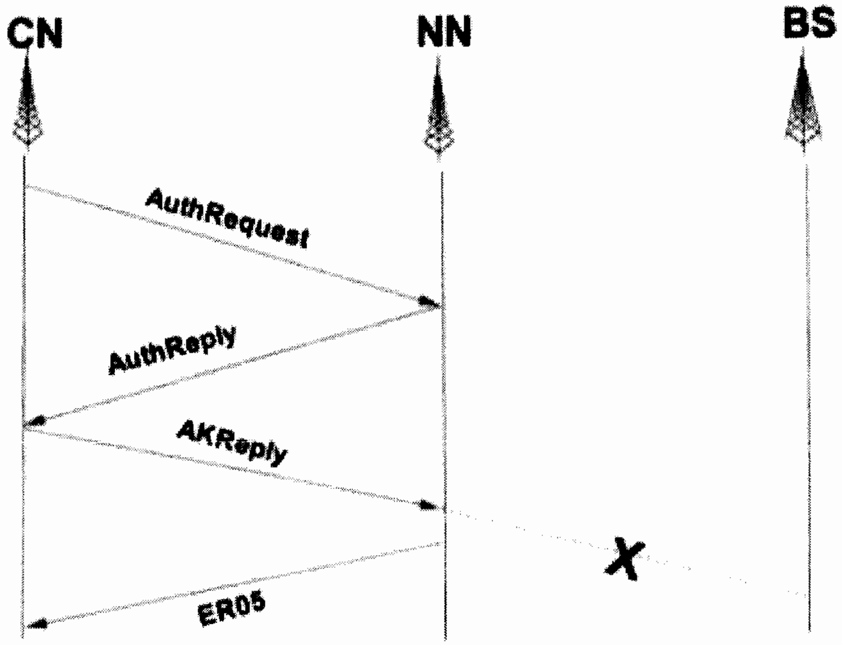

Figure 16: Disconnected from the BS in Authentication Key Request

Case-6 ER06 (Invalid Sequence No)

CN → NN : AuthRequest

NN→CN : AuthReply

CN→NN: AKRequest

NN→BS: AKRequest

BS→NN: AKReply

NN→ CN : AKReply

CN→NN: TEKRequest

NN→BS: TEKRequest

BS→NN: ER06

NN→CN: ER06 (Invalid Sequence No)

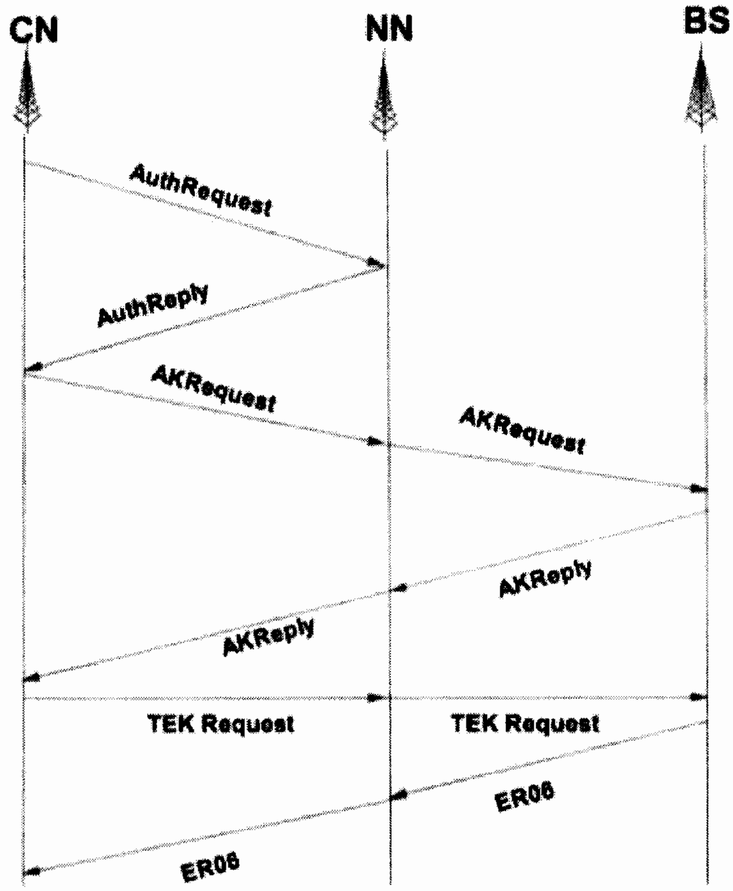

Figure 17: Invalid SeqNo from the Candidate node in Authentication Key Request

Case-7 ER07 (AK Expires)

CN → NN : AuthRequest

NN→CN : AuthReply

CN→NN: AKRequest

NN→BS: AKRequest

BS→NN: AKReply

NN→ CN : AKReply

CN→NN: TEKRequest

NN→BS: TEKRequest

BS→NN: ER07

NN→CN: ER07   (AK Expires)

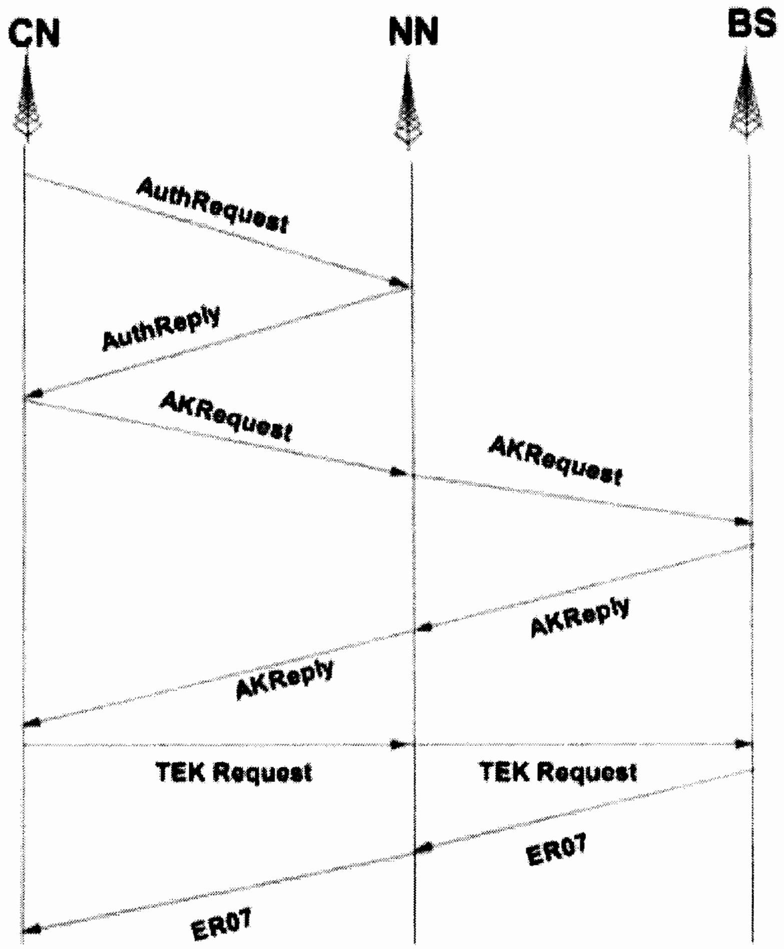

Figure 18: AK Expires request from candidate for TEK

Case-8 Keys Granted

CN → NN : AuthRequest

NN→CN : AuthReply

CN→NN: AKRequest

NN→BS: AKRequest

BS→NN: AKReply

NN→ CN : AKReply

CN→NN: TEKRequest

NN→BS: TEKRequest

BS→NN: TEKReply

NN→CN: TEKReply (TEK Grranted)

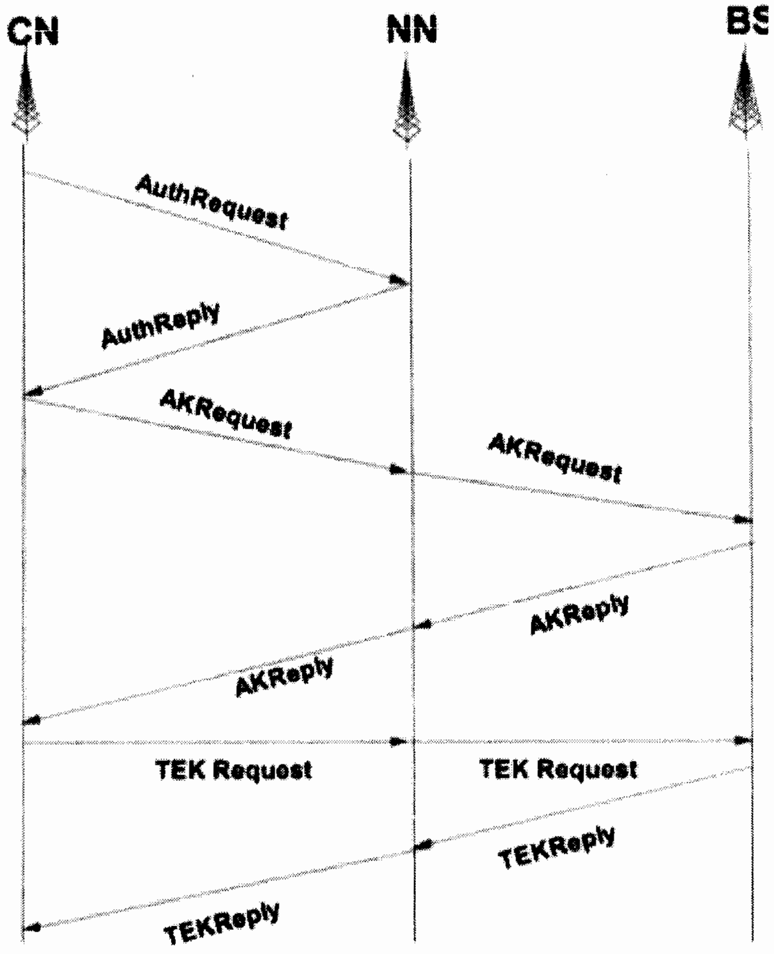

Figure 19: Keys are Granted

5.3 Algorithm / Pseudo code

The pseudo code of the three communicating nodes BS, NN, CN involved in our protocol is as;

BS (server always in listen mode)

```
{
Check whether Requester is requesting for Authentication
Then jump to 1:
OR
Jump to 2: (For Traffic encryption Key)

1:
        {
        Receive request from the NN (for the authentication)
        Accept this request.
        Issue AK and also keep record of it.
        Reply it by sending the Pre AK, BCID (IP) and Seq no (for AK generation at CN)
        to the NN.

        }

2:

    {

    Receive the request for TEK
    Verify the Authentication Key from its record
    Accept the request
    Reply it with old and new TEK encrypted with CN public key

    }

}
```

NN (intermediate node in listen mode)

```
{
Check request by using authentication level
1: For authentication of using temporarily channel
2: For authorization Key

1:
        {
        Accept the request
        Verify the certificate, TKN to avoid reply
        Reply to requesting CN
        }

2:
        {

{
Receive request form the CN
Accept the request.
Reply this to CN by including its own identity.
}
CN again request for the authentication key.
NN forwards this request to the authorization node.
Authorization node replies this request to NN and then NN finally hand over this message
to CN.
Connected
}
```

CN (node that was requesting for the authentication)

```
{
{
1. Send request to neighbor for mutual authentication by sending its certificate.
2. Receive reply from the neighbor with information (TKN, Cert(NN), SIG NN)
}
3. Request accepted by the neighbor node for providing the temporary channel.
4. Send request to the BS through neighbor having (nonce CN, Certi CN,TKN, etc, SIG CN)
5. Neighbor receive this message and forward it to the BS (authorizing node) by Adding its own signatures now the message becomes (previous at step 4, SIG NN (NN remove the signature of CN and add its own))
6. NN receive reply from the BS including (message at step 5, nonce BS, SIG BS , SEQ no, Pre-AK encrypted with CN Public key).
7. NN forwards this message to the CN by adding its own SIG with message at step 6.
8. CN authenticated and can use the services of the network. But before using the service CN must take traffic encryption key from the BS.
9. CN sends the request for traffic encryption key (Information encrypted with private key)
10. NN forwards this request to   BS by adding its own signature.
11. BS reply with TEK encrypted with public key of CN to NN
12 NN forward this information to CN.
13 now CN can fully participate in mesh.

}
```

5.4.1 Classes and their Method:

Following classes are involved in the developed system.

Classs BSStarter

Methods:

Start() Creates and start an object of BaseStation class. This will be used to run the base station that starts listing requests from neighboring nodes for authentication.

Class BaseStation

Methods:

startService() Method that create a server port and get local IP and MAC address and finally star running BS for requests for NN and CN.

processMessage()

Process messages that are exchanged between BS, NN and CN respectively.

stopService() Stopping BS from listening requests.

void run() Restart the BS in the listening mode.

Class BSPoint

Methods:

run() Loading BS certificate and also authenticate it.

readRequest() Reads NN request

writeReply() Reply NN request

getAK() Creates AK and return it to the requesting one

readCert() Read the certificate

isLoadCerts() Checks whether the certificates has been loaded successfully

Class **NNStarter**

Methods:

Start() Creates and start an object of NeighboringNode class. This will be used to run the neighbor node that starts listing requests from new nodes for authentication.

Class **NeighbourNode**

startNode() Get thc IP and MAC of thc BS and start listening requests from CN

joinBaseStation() Connect neighbor node with the base station when connection is successfully completed.

writeMessage() Sends information message to BS

class **Endpoint**

authenticate ()	Authenticate requests from CN
writeCert()	Write certificate information to a file
readCert()	Read certificate data
run()	Checks if the certificate is loaded successfully and also start authentication

Class **CNStarter**

Methods:

Start() Creates and start an object of CandidateNode class. This will be used to run the candidate node requesting NN to forward request to BS

Class **CandidateNode**

authenticate () Sending authenticating credentials to the NN and wait for NN response.

joinNN() Send a joining request to NN.

joinBS() Joining request to BS

getSecretKey Get secret key information

Class **Constants**

Methods:

loadConstants() Load all the values that remain constants through out the session.

5.5 Summary

This chapter focuses on the implementation phase of the research. It lists the tools and technologies used to develop the proposed system. The system flow diagram describes the flow of data at each step. Then pseudo code and algorithm of the system is also defined in detail. Finally this chapter contains the list of classes and method involved in the implementation. The next chapter discusses the testing and performance evaluation of the proposed system.

6. Testing and Performance Evaluation

6. Testing and Performance Evaluation

Since the hardware requirement for implementation of the proposed system are not freely available. We use mathematical model to prove our work. In mathematical model we take some values in both the scenarios for existing protocol and the proposed protocol. In some extent it is proved that the proposed scenario is better that that of the previous. We used hybrid approach in the proposed protocol. In our proposed hybrid approach Spoofed requests are controlled, reply attack is mitigated, Avoided flooding, Jumping Forward is controlled, Man in the middle attack is removed ,Improve Service Delivery, Reduce the authentication packet size, Bandwidth is saved , Inexpensive in processing and Inexpensive in power consumption. In the proposed system intra-communication between the nodes can not disturb the BS. In the previous key management protocol hash function is used which is expensive in computing, power consumption and may cause the denial of service for the nodes. We replace it with signatures which also increase the processing capability of the BS.

6.1 Test Scenario

WIMAX-based mesh deployment scenarios are considered. In the mesh every SS can directly communicate with other SS after authentication process is successfully completed. Mesh BS partially manages communicating nodes. Mesh BS plays the role of passing necessary information to the external network. When any node joins the mesh network authentication and authorization is performed by the neighboring or sponsoring node. Mesh.

6.2 Performance and Evaluation

Our proposed system has following advantages over the previous work.

1. Spoofed requests are controlled
2. Avoid the reply attack
3. Avoid flooding
4. Jumping Forward is controlled
5. Man in the middle attack is removed
6. Improve Service Delivery
7. Reduce the authentication packet size

8. Bandwidth is saved
9. Inexpensive in processing
10. Inexpensive in power consumption

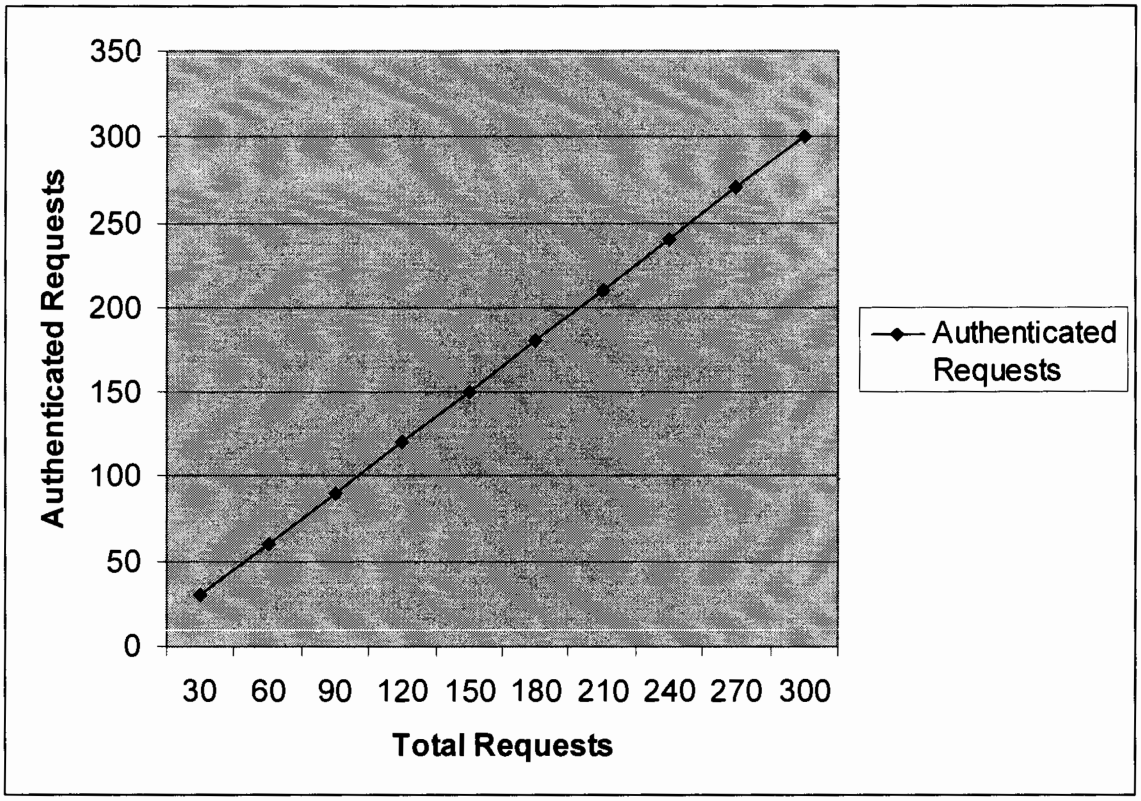

Figure 11: Authentication of Legitimate Requests

First we check our system for the legitimate requests. In this case we send all legitimate requests to check whether our systems authenticate all legitimate requests or it may also stop some legitimate requests. We send three hundred legitimate requests and all are authenticated as shown in the figure 11.

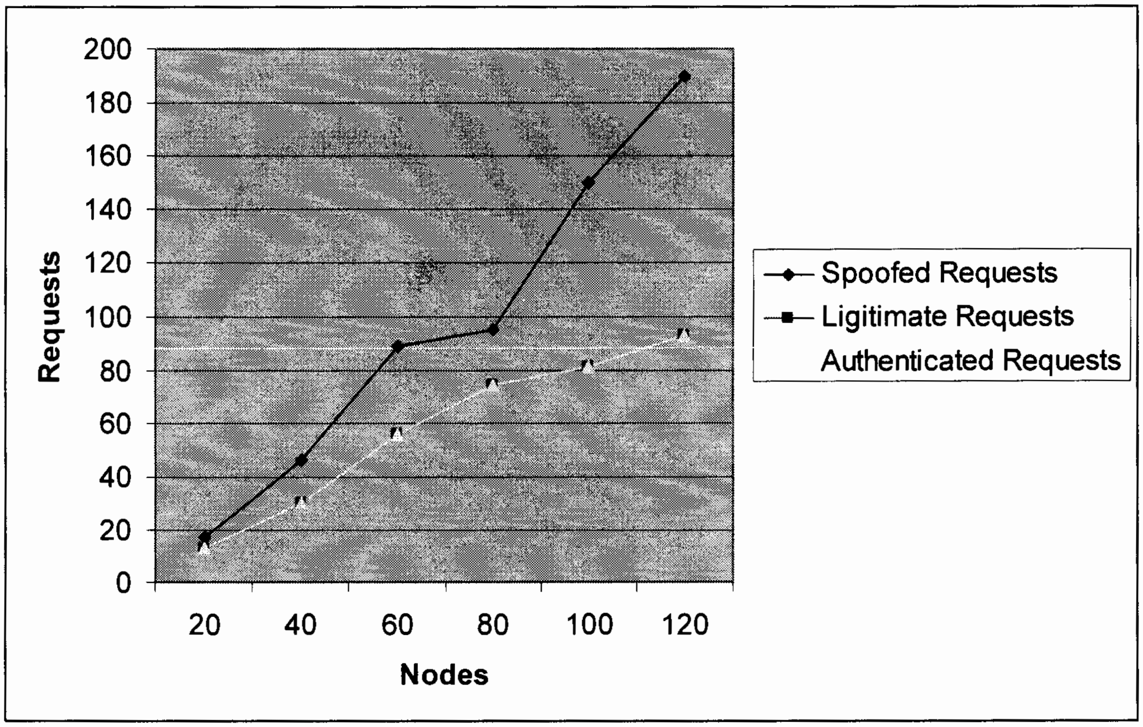

Figure 12: Spoofed and Legitimate Requests

In the second scenario we check our developed system for the mixed requests which includes legitimate and spoofed requests. In this case we send 190 spoofed and 90 legitimate requests in a mixed mode figure 12 shows that developed system authenticate all the 90 legitimate requests only. System discard all the spoofed requests.

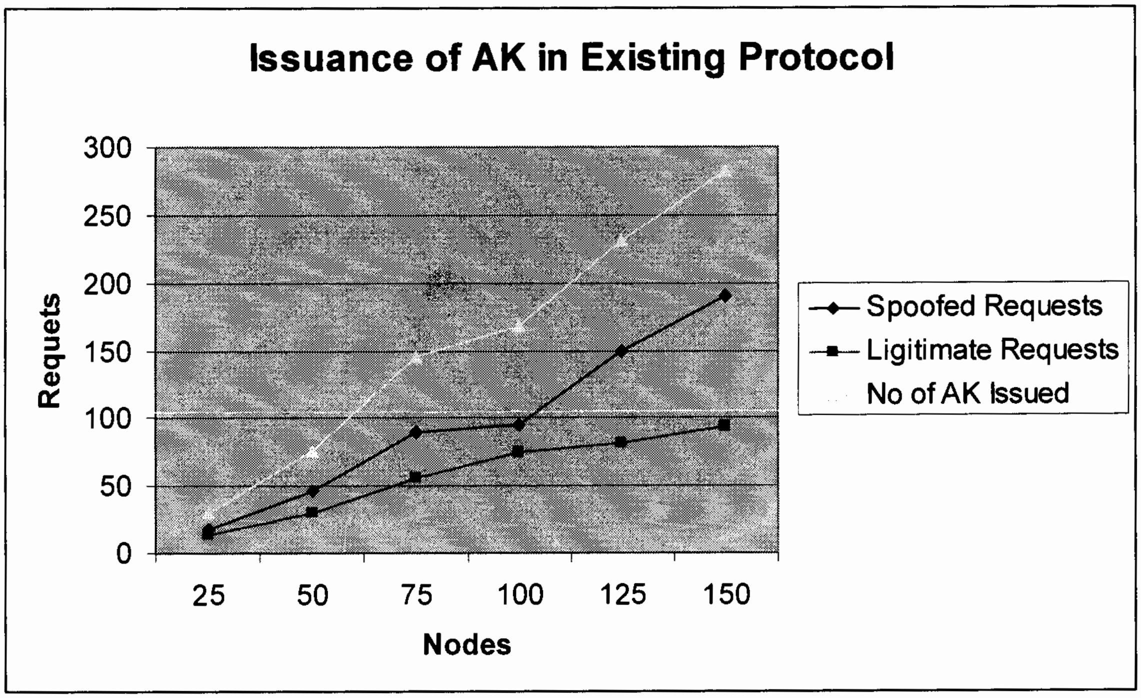

Figure 13: Issuance of AK in Existing Protocol

Figure 13 shows the issuance of authentication key in case of the existing protocol. In this case we send mixed requests on the existing authentication protocol 190 spoofed and 100 legitimate but the existing protocol issue 290 authentication keys .

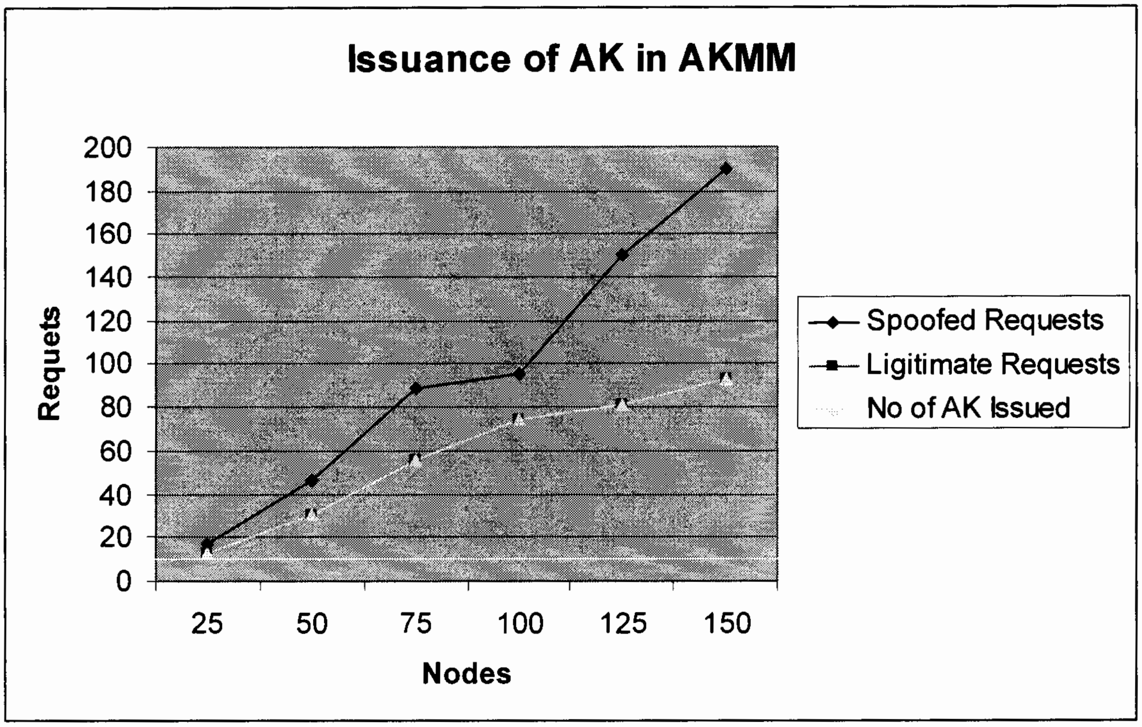

Figure 14: Issuance of AK in AKMM

In the proposed protocol same number of authentication requests are send as that in the figure 13 for authentication but it issue the authentication keys to the legitimate requests only and discard all the spoofed requests as shown in the figure 14 which remove extra burden of processing from the BS/Authentication server.

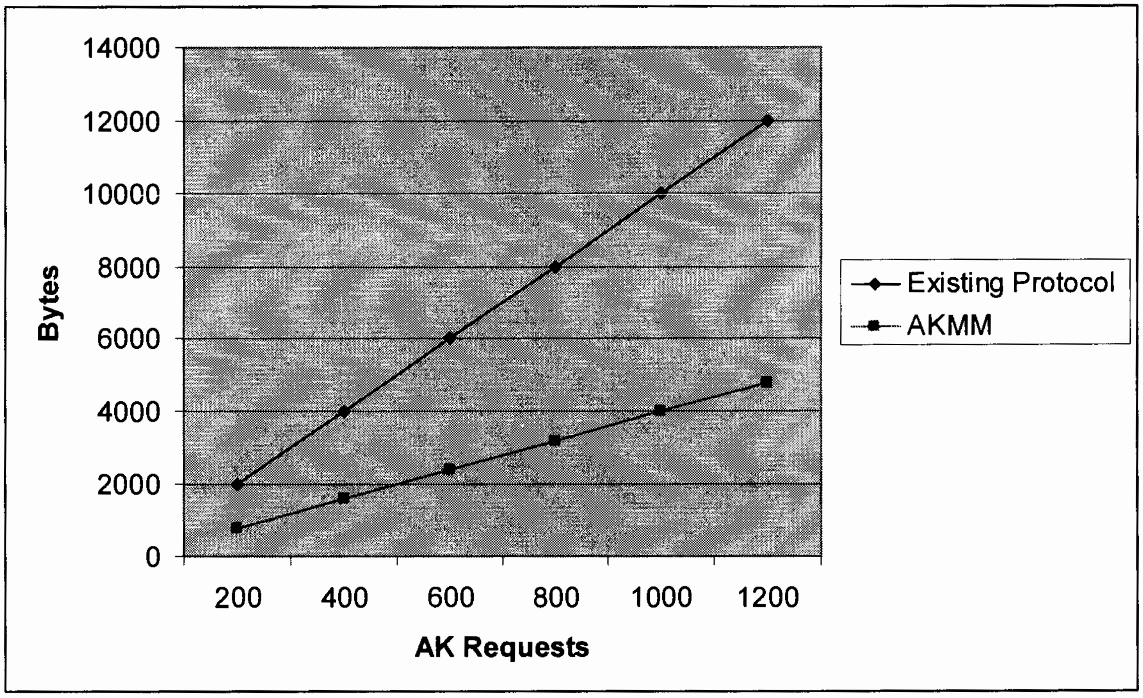

Figure 15: Payload Comparison of messages in AK Requests (common fields are omitted)

The graph shows the data comparison of the two protocols in case of authentication requests, graph shows that the proposed protocol has fewer amounts of data which is attached along with payload from CN to BS. So the message size for our protocol is lighter as compared to previous one.

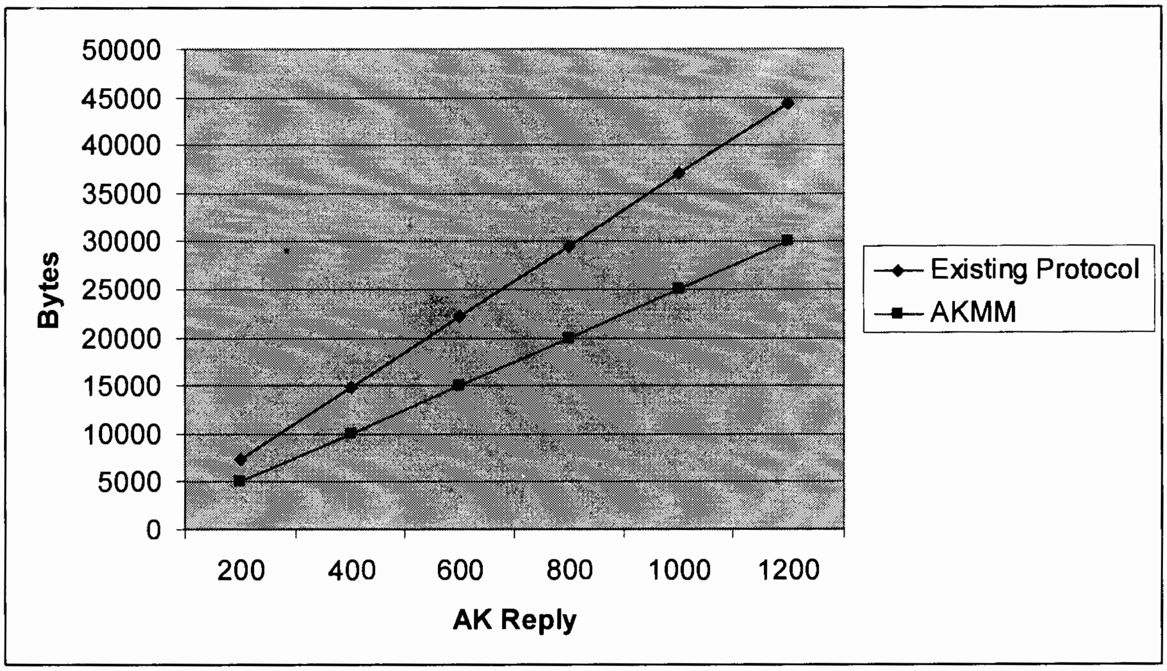

Figure 16: Payload Comparison of messages in AK Reply (common fields are omitted)

The above graph shows the message size comparison in case of authentication reply proposed protocols have lesser size as compared to the previous protocol.

6.2.1 Comparison of AKMM and Existing Protocol

Comparison of our protocol and the existing protocol is shown below;

Sr. No	Features	AKMM	Existing Protocol
1	Spoofed Requests	Controlled by Token	Possible to Launch
2	Replay attack	Avoided through Authentication Level	Possible to Launch
3	Malicious Neighbor node	Controlled through mutual authentication	Can be possible
4	Jumping forward	Controlled by Authentication Level	Jumping forward can not be controlled
5	Water Torture Attack or Flooding	Controlled through Authentication level	Can be possible
6	Man in the middle Attack	Controlled by Mutual authentication	Can be possible

Table: Comparison of AKMM and Existing Protocol

\

6.2.2 Comparison of AKMM and Existing PMP Protocol

Sr#	Features	AKMM	Existing Protocol
1	When authentication requests become numerous	Easily Handled because BS/Authorization node have less load	Drop some requests due to heavy load on single BS/authorization node
2	Processing and power consumption	BS/Authorization node required less processing	BS/Authorization node have to process all the requests which requires more processing and power

Table: Comparison of AKMM and Existing PMP Protocol

6.3 Summary

This chapter focuses on the testing and performance evaluation of the proposed protocol. First it briefly discussed the working environment of the proposed system. Then test scenario is mentioned and at the end results of previous system and proposed system is compared and theses results are expressed in form of graphs. In the next chapter we give the concluding remarks and finally proposed some future recommendations.

7. Conclusion and Outlook

7. Conclusion and Outlook

WIMAX is the broadband technology that is used to for high connectivity over long distances, it is also becoming more powerful for Internet and telecommunications service providers. This emerging standard for wireless communication is designed by the IEEE 802.16 experts; WIMAX has been launched after the security failures of the IEEE 802.11 networks. WiMAX is more secure than the existing wireless technology but has been found many shortcomings.

A basic flaw in WIMAX's privacy and key management (PKM) protocol is the lack of base station (BS) or service provider authentication, which is necessary for such kind of wireless networks. This lack makes WIMAX networks vulnerable to man-in-the-middle attacks, DoS attacks jump forward attacks etc. Since the management frames of 802.11 specifications are not encrypted, which allow attackers to gather information about subscribers in the area and some sensitive information can also be compromised. Many other attacks from attackers, including Rogue base stations, DoS attacks, Man-in-the-middle attacks, authentication attacks, Attacks related to spoofed management frames can also be launched. A large number of PKM related problems are also present in the standard.

There were many security threats that the users can face. Security of WiMAX mesh is a hot issue these days in wireless communication especially in mesh networks. Possible threats exist like Replay Attack, DoS Attack, Jump forward Attack and BS/SS masquerading etc. Because of these security threats a secured authentication and key management protocol is proposed to solve the said security problems along with key issuance and management.

In IEEE802.16e added support for the Extensible Authentication Protocol (EAP) to WIMAX networks which will be helpful for end-to-end authentication. The PKMv2 solves the BS authentication which was a problem in WiMAX, is solved by mutual authentication.

Thus the main objective the thesis is to study the WIMAX authentication and key management protocol, security architecture, encryption schemes used, try to find the limitations while implementing this protocol in mesh mode and try to remove the limitations in authentication and key management process by introducing a new authentication and key management protocol for mesh networks.

7.1 Achievements

When we start working on the thesis, we examined that 802.16 is possible to be vulnerable. Still, such vulnerabilities are theoretical, which is based on a paper assessment. When the standard's equipment will be available, such vulnerabilities will be verified that exists. If these may exist though, it will not be possible for an intruder or attacker to exploit them. However, even though it is much more difficult, it takes single person to exploit it. Since the standard evolves, the possible threats are fixed, but new threats may arise that will damage the system security.

Our proposed protocol will improve the security of WiMAX as well as the authentication and key management for the new node that want to join the mesh network.We hope that our proposed protocol will get success when we talk about the security of IEEE WiMAX standard. All types of security threats which we presented will be solved.

By using proposed technique secure communication can be possible, no malicious SS can participate in the mesh network, replay and jump forward attacks will also be minimized. Thus BS bandwidth can be used in a more affective manner.

7.2 Improvements

Following improvements have been observed

1. Authentication of Candidate Node and Neighboring Node
2. Replay attack Mitigation.
3. Jump forward attack Mitigation.
4. Spoofed requests handling.
5. Secure uplink and downlink communication in Mesh
6. Comparative lesser resource consumption.
7. Eliminated duplicate entries at BS.
8. No synchronization required between the nodes.
9. Flexible
10. Fault Tolerant

7.3 Future Recommendations/Outlook

In this thesis we propose an Authentication and a Key management protocol for WIMAX mesh networks. In this protocol authentication of new node is done at entry level by neighboring node in the mesh. The key issuance authority is BS. After the authentication new node requests for the keying material. This technique is useful for mesh it can be further improved. More research is needed in session management and issuance of authentication key by the BS in WIMAX mesh architecture.

7. 4 Summary

This chapter contains the final concluding remarks of the research work. In first section, we briefly describe the need of the new technology and improvements in its authentication and key management protocol. We also describe some security restrictions in the existing protocol and propose a new protocol for the WIMAX mesh. In the next section we states achievements which we obtain from the proposed work but most things are theoretical due to lack of implementation of WIMAX standard. Finally we propose a number of recommendations and directions which require more concentration in the future.

References and Bibliography

[1] Fan Yang, Huaibei Zhou, Lan Zhang, Jin Feng “An improved security scheme in WMAN based on IEEE standard 802.16” a paper published in IEEE on 2005.

[2] A White Paper “IEEE 802.16a Standard and WIMAX Igniting Broadband Wireless Access “www.wimaxforum.org”

[3] David Johnston, Jesse walker “overview of WIMAX security” published in IEEE in 2004.

[4] “Security issues in privacy and key management protocols of IEEE 802.16” published in ACM journal in March, 10-2006.

[5] Michel Barbeau “WiMAX/802.16 Threat Analysis” presented in Q2SWinet ’05, October 13, 2005, Montreal, Quebec, Canada.

[6] Ron Olexa “Implementing 802.11, 802.16 and 802.20 wireless networks”.

[7] Asad Amir, Marius Portmann and Jadwiga Indulska “Evaluation of Multi-radio extensions to AODV for wireless mesh networks” published in ACM in Oct, 2006.

[8] IEEE Std 802.16a-2003, "IEEE Standard for Local and metropolitan area networks--Part 16: Air Interface for Fixed Broadband Wireless Access Systems--Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz," 2003

[9] Hung-Yu Wei, Samrat Ganguly, Rauf Izmailov Zygmunt J. Haas “Interference – Aware IEEE 802.16 WIMAX Mesh Networks” published in June 2005.

[10] IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004.

[11] W.A. Arbaugh, N. Shankar and Y.C Wan “your 802.11 network has no cloths” published in March 2001.

[12] “Mobile Broadband Wireless Access” by Samiseppo Aarnikoivu, Juha Winter published in april 2006.

[13] Leiner, B. M., Cerf, V. G., Clark, D. D., Khan, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S. S. (1997). The Past and Future History of the Internet. Communications of the ACM, 40 (2), 102-108.

[14] Internet Systems Consortium. (2005). ISC Internet Domain Survey. [On-line]. Accessed on February 5, 2006 at

URL:http://www.isc.org/index.pl?/ops/ds/host-count-history.php.

[15] Intel Corporation. (2004). Understanding Wi-Fi and WiMAX as Metro-Access Solutions. [On-line]. Accessed on September 25, 2005 at

URL:http://www.intel.com/netcomms/technologies/wimax/304471.pdf.

[16] IEEE 802.16 Working Group. (2002). IEEE 802.16 Backgrounder. [On-line]. Accessed on January 29, 2006 at URL:http://ieee802.org/16/pub/backgrounder.html.

[17] IEEE 802.16 Working Group. (2004). PAR 802.16f. [On-line]. Accessed on January 29, 2006 at URL:http://grouper.ieee.org.csulib.ctstateu.edu/groups/802/16/docs/04/80216-

04_34r4.pdf.

[18] http://standards.ieee.org/getieee802

[19] www.wikipedia.org

[20] Eric Kaasenbrood, "WiMAX Security – A Formal and Informal Analysis", Technische Universiteit Eindhoven, Masters Thesis, August 2006

[21] Sen Xu et.al. "Attacks on PKM protocol of IEEE 802.16 and its lator versions"

[22] I. F. Akyildiz and X. Wang. A Survey on Wireless Mesh Networks. IEEE Communications Magazine, 43(9):S23–S30, 2005.

[23] Bongkyoung Kwon et.al " a Security Scheme for Centralized Scheduling in IEEE 802.16 Mesh Networks". IEEE Communication Magzine, 2007.

[24] Yun Zhou and Yauguang Fang "Security of IEEE 802.16 in Mesh Mode". IEEE Conference on Military Communication ,Oct 2006.

Acronyms

AES:	Advanced Encryption Standard
BS	Base Station
BWA	Broadband Wireless Access
CDMA	Code Division Multiple Access
CN	Candidate Node
CPE	Customer Premise Equipment
DL	DownLink
EAP	Extensible Authentication Protocol
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronic Engineers
LOS	Line-Of-Sight
MAC	Medium Access Control Layer
MAN	Metropolitan Area Network
Mb/s	Megabit Per Second
NLOS	Non-Line-Of-Sight
PDU	Protocol Data Units
PHY	Physical Layer
PKM	Privacy and Key Management
PKMv2	Privacy and Key Management Version 2
PMP	Point-To-Multipoint
PPP	Point-To-Point Protocol
QoS	Quality of Service
SAP	Service Access Points
SS	Subscriber Station
TDD	Time Division Duplex or Duplexing
TDM	Time Division Multiplexing

TDMA	Time Division Multiple Access
UL	UpLink
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WMAN	Wireless Metropolitan Area Networks