IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 3, Ser. III (May - June 2019), PP 10-15
www.iosrjournals.org

Study of PKM Protocols and Threats in Wimax

Rajesh Kumar[1], Rabira Geleta Ibsa[2], Negasa Berhanu[3], Abdirkadir Hassen[4].
[1](Department of Computer Science, College of Informatics /Bule Hora University,Ethiopia).
[2](Department of Computer Science, College of Informatics /Bule Hora University,Ethiopia).
[3](Department of Computer Science, College of Informatics /Bule Hora University,Ethiopia).
[4](Department of Computer Science, College of Informatics /Bule Hora University,Ethiopia).
Corresponding Author: Rajesh Kumar

Abstract: *WiMAX provide the fixed and wireless connectivity to the MS and SS node in metropolitan environments. For the wireless environment, security is very main concern because security is more compromised as compared to wired network. Therefore privacy key management protocols are designed to secured key exchange and management of the security in wireless environment in WIMAX. These PKM protocols have many flaws and weakness. An attacker can try various attacks on these protocols to break the confidentiality, integrity, authentication and authorization. There are two main protocol pkmv1 and pkmv2. This paper constitutes the study of these protocols and find out the various threats possibility in the both protocol version.*

Keywords: *AK, MITM, SAID, TEK, KEK*

Date of Submission: 09-05-2019 Date of acceptance: 25-05-2019

I. Introduction

During last some year wireless is very popular and changes our life styles. Whenever the need arises of mobile networks thinking about mobility, user practices it in office, home, while travelling, and research organizations. Currently research going in wireless area to increases mobility, coverage area, security and maintain the quality of service requirements. WiMAX (Worldwide Interoperability for microwaves access) assign IEEE 802.16 standards official known as Wireless MAN [1]. WiMAX is the future growing technology working in the area of telecommunication suitable for 4G network to provide high broadband service to the user. IEEE Standards Board Established in 1999, the IEEE 802.16 is a working group on Broad Wireless Access (BWA), developing standards for the global deployment of broadband Wireless Metropolitan Area Networks .In December 2001, the first 802.16 standard which was designed to specialized point to multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light-of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications [2]. Therefore after 2003 the first standard IEEE 802.16a who fulfill the requirement of LOS and NLOS is published. It has two main standards IEEE 802.16d for fixed WiMAX network and IEEE 802.16e for Mobile WiMAX network published in the year of 2004 and 2005. The third standard (IEEE 802.16m) is also published; WiMAX forums research is going on this area. Security becomes the prime concern in WiMAX to provide protected communication. WiMAX wireless interface threats focus on compromising the radio links between WiMAX nodes. These radio links support both line-of-sight (LOS) and non-line-of-sight (NLOS) signal propagation. Links from LOS WiMAX systems are generally harder to attack than those from NLOS systems because an adversary would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link. WiMAX NLOS systems provide wireless coverage over large geographic regions, which expand the potential staging areas for both clients and adversaries. Like other networking technologies, all WiMAX systems must address threats arising from denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation [3]. Therefore two privacy key management protocols PKMv1 and PKMv2 was design in WiMAX to provide the protected communication between nodes. In the second section on this paper discuss about security protocol Pkmv1 and their detail description, the section third about the Pkmv2 protocol and their details description, section fourth constitute the various attacks possibilities in Pkmv1 protocol and Pkmv2 protocol, section fifth is conclusion about this paper.

II. Overview Of Pkmv1 Protocol

Privacy Key Management Version 1 (PKMv1) [IEEE.802.16-2004] is a public-key-based authentication and key establishment protocol that is typically used in fixed wireless broadband network deployments. The protocol utilizes X.509 v3 certificates, RSA encryption, and a variety of secret key cryptographic methods to allow an 802.16 Base Station (BS) to authenticate a Subscriber Station (SS) and perform key establishment and maintenance between an SS and BS [4]. The phase of PKM (Privacy key management) shown in fig. 1.

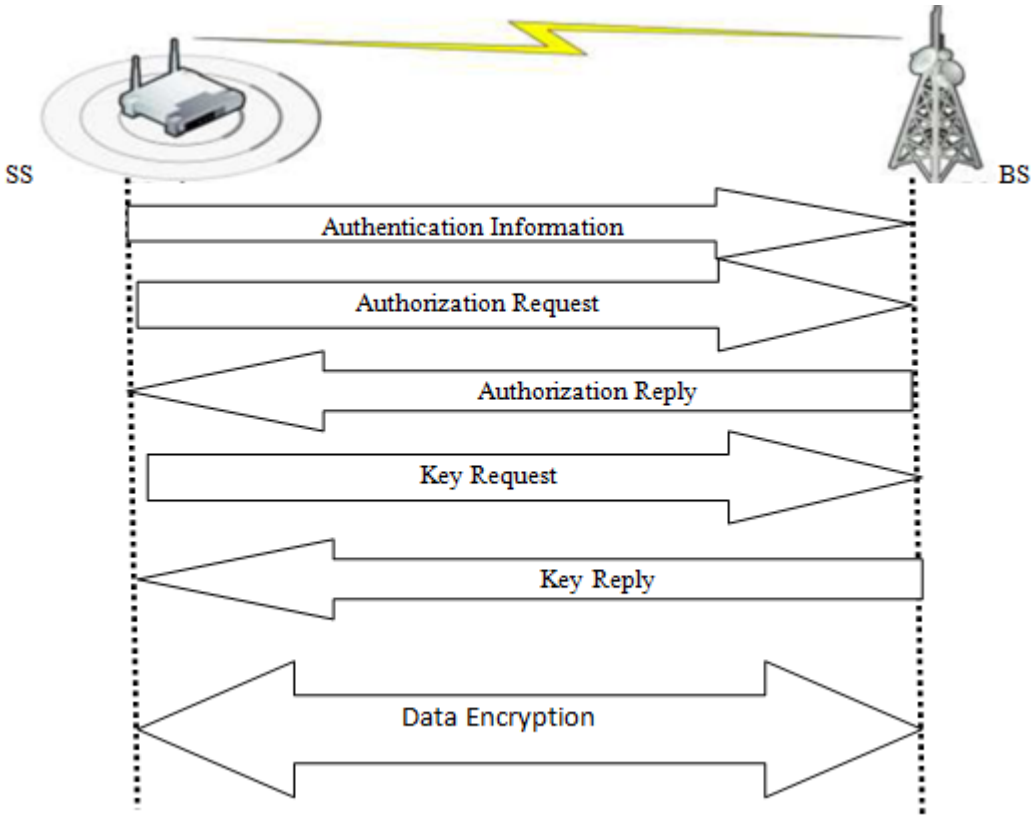

Fig: 1- PKM protocol Phase

PKMv1 provide one-way authentication means that the only authorization process is initiated form the Subscribe Station not from BS. The authorization process is initiated when the SS sends an authorization information message to the BS (Figure-2). Immediately following the authorization information message, the SS sends an authorization request to the BS, which contains the following information:

- The SS's unique X.509 certificate, which includes its RSA public key.
- A description of the SS's supported cryptographic algorithms.
- The primary 16 bit SAID (Security association identifier).

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

- The activated AK(128 bit), encrypted with the SS's public key
- The AK sequence number used to differentiate between successive generations of AKs
- the AK lifetime
- A list of SAIDs that the SS is authorized to access and their associated properties.

The reauthorization process is identical to the initial authorization process with the exception that the authorization information message is not re-sent [5].

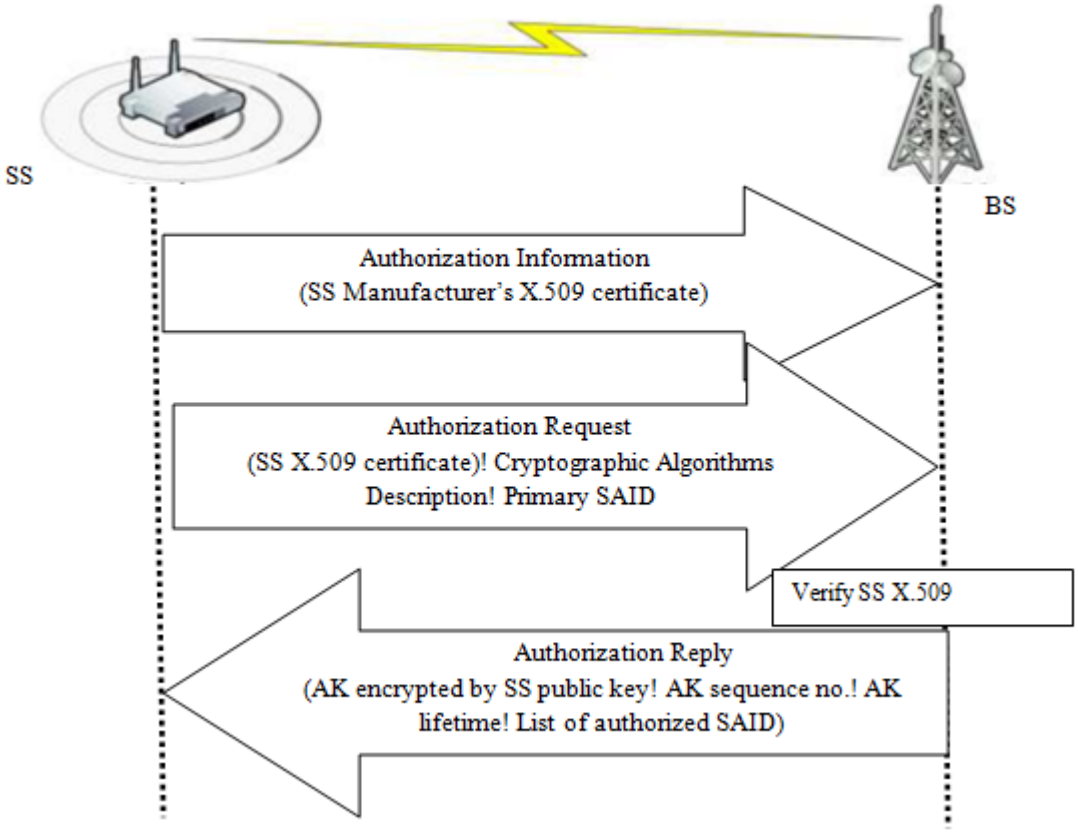

Fig.-2 PKmv1 Authorization

III. Overview Of Pkmv2 Protocol

As discussed in the previous section the version 1 protocol is provide only one way authentication. The version 2 protocol has more security features and it does provide different type of authentication mechanism, one is RSA based authentication and another one is EAP (Extensible Authentication Protocol) based authentication.

There are following security features available in Pkmv2 protocol:

Privacy and key management protocol: Pkmv2 protocol managing the MAC security using TEC (traffic encryption control). TEC will control all the handover key exchange and all related security message that are going to use in initial authentication and authorization mechanism.

User authentication: the protocol support device authentication using EAP by providing feature whether it is SIM based authentication, user name or password based or certification based authentication.

Traffic Encryption: it is provide strong encryption of the user data using cipher technique and EAP based key generation for providing data safety and the traffic encryption state machine that key are derived using TEK and also have suitable refresh mechanism.

Fast Handover Support: three way handshaking provide re-authentication mechanism quickly so that the fast handover mechanism can be achieved. [5]

To overcome the mutual authentication problem, the protocol provides two ways authentication mechanism both SS and BS mutually authenticate itself. The protocol use RSA algorithms for key exchange, MS established it identity using manufacturer digital certificate (X.509) or using subscriber module identity (SIM) card. This certificate (mobile station public key and mac address) is transfer to certificate authority for validation purpose. The CA verifies the certificate and validates the mobile station identity. After validation of the user identity it is going to create authorization key by use of public key and this authorization key is used by MS and BS to derive another encryption key that is going to use by AES algorithms [6].

The initial RSA authentication and key generation and management process done by the following steps:-

Initially mobile station sends a message (authentication information messages) to the BS. Massage have X.509 certificate of the MS. In another message MS send RSA request message (Pre-Pak and Saids) to the BS. This message contains X.509 certificate, Algorithm details used for Cryptography, Basic CID of MS and 64 bits random number.

Base Station Act after receiving this message

- It authenticates the Identity of the MS, find out the protocol types and encryption algorithms trigger Pre-Pak for the mobile stations encrypt using the public key of the mobile station.
- RSA Reply messages, BS send a RSA reply message have the following information,
  BS certificate for his own identity, Pre-Pak(Pre-Privacy Authorization key) encrypted with public key of the MS, 4 bits PAK sequence no, PAK lifetime, SAIDs(Security Association Identifiers), 64 bits random no. received from MS and his personal 64 bits random no. , RSA signature on other elements of this message.
- MS and BS derived key independently, the PAK from received Pre-PAK, AK from derived PAK, KEK and HMAC/CMAC key from derived AK.
- Next BS sends a SA-TEK challenges message to the MS. To find out whether the MS have a valid Authorization key (AK) or not. MS send SA-TEK request message to request the base station to generate a TEK and send it to back.
- In reply BS generate a TEK encrypt using KEK, send the encrypted TEK to MS in SA-TEK response Message. MS decrypt the TEK and use it for Encryption and Decryption for upcoming traffic.

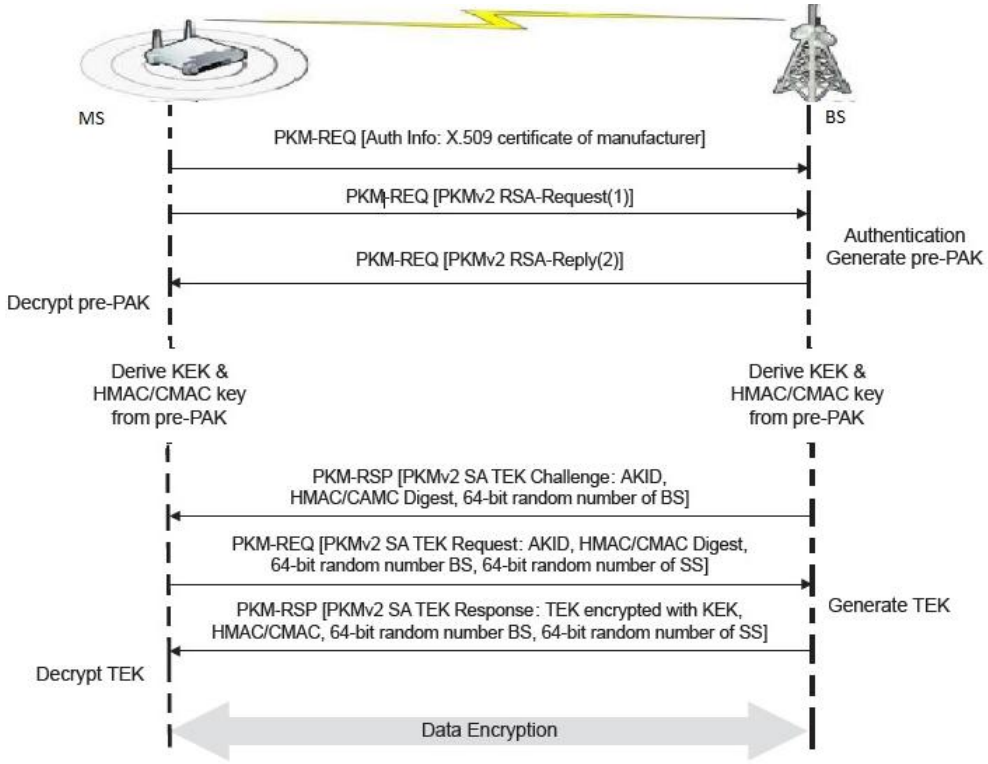

Fig-3 Initial RSA Authentication and Key Generation and Management Process

There are other scheme of key authentication and authorization except RSA: EAP based authorization, RSA followed by EAP base authorization, EAP followed by EAP based authorization (double authentication mechanism) are limited scope in this paper. All schemes are followed by mutual authentication mandatory [7].

Authentication and Authorization in PKMv2

Mutual Authentication: PKMv2 introducing mutual authentication, giving both stations the possibility to check each other's identity.

Authentication of User Data: AES in CCM-Mode

Control Message Protection: AES based CMAC, or HMAC schemes

Authorization: generation of the Authorization Key (AK) within the Authorization Phase leads to a higher security level.

IV. Various Threats On Pkmv1 And Pkmv2 Protocol

The PKMv1 protocol is vulnerable to so many threats. The details description of various attack are given below:

1. Message replay attack

The message carries from SS to BS have one way mutual authentication, if the message travel from SS to BS does not carry the proper freshness identifiers, the bogus SS can authenticate himself from the BS and communicated with BS using legitimate authentication message. This type of attack called Message replay attack. A malicious SS can capture the original message sequence and replay the message to BS for authenticate himself. It can be avoided if the proper freshness identifier sequence will be travel from SS to BS.

2. Man in Middle Attack

There is only one way authentication IN PMKv1 protocol only the SS is authenticated by the BS. BS is not going to authenticate by SS. So a forging BS can register himself to communicate with SS. And SS don't have any way to identifies whether the given BS is falsifying or legitimate. This type of attack called MAN in Middle attack. It can be avoided by two way authentication.

3. Eavesdropping Attack

DES is consider Insecure, for encrypting transmission of the traffic, Pmkv1 only supports the use of DES-CBC, which has well-documented weaknesses and is no longer approved for Federal agency use in protecting communications. The DES standard has breach of confidentiality, so the eavesdropping attack is possible. So it no longer recommended using DES –CBC mode of Encryption. Unencrypted management messages -the management message are also not encrypted which lead to confidentiality breach and eavesdropping, DOS, replay attack possibilities will be present.

4. DOS Attack

The initial network entry process is the main process to establish a connection to the network. When SS first tries to join network, it sends a Ranging Request message. BS sends a Ranging Response to SS for various parameters. The attacker can capture this RNG-RSP message and send the spoofed RNG-RSP message by setting the RANGING_STATUS value to 2 which means "abort", the author suggest to a DoS attack [8]. All wireless communications are susceptible for radio frequency jamming attack. This is the kind denial of service attack; the threat arises from a foe hosting a powerful RF signal to beat the spectrum being used by the system, thus author justify denying service to all wireless nodes within range of the interference [3]. The jamming can be prevented increase the power level using FHSS and DSSS. The management frames in WiMax are similar to WiFi's. In wi-fi disturb the service of the two communicated nodes, which related to DOS attacks, Wi-Max has cryptographic protections from spoofed identities, but replay DoS attacks still remain a threat to WiMax, due to the lack of any mechanisms to specifically detect and discard repeated packets.

5. Masquerading attack

The masquerading threat of the BS or SSs is enabled when authentication weaknesses are present. In pmkv1 SS only authenticate to BS, in no way BS can authenticate to the SS. Identity theft and Rogues BS are specific techniques of masquerading. A forged device can use the hardware address of another registered device by capturing management messages over the air. Once succeeded, an attacker can turn a BS into a rogue BS. A rogue BS can imitate a legitimate BS by confusing the associated SSs. Those SSs try to acquire WiMAX services from the rogue BS, resulting in degraded service or even service termination [6].

Threats on PKMv2:

This version protocol provides a three-way authentication with a confirmation message from SS to BS. But there is lack of integrity and no-repudiation in authorization process of this protocol. In the Authorization request/reply message, if the interceptor properly sited radio receiver catches the message, the lack of digest method prove that the messages have not been changed by others and nothing is used to make sure the sender cannot repudiate the message. Without the use of SS signature an attacker can forge new frames and capture, modify, and retransmit frames from authorized parties.

1. Simple Replay attacks and Interleaving attack:

A replay attack possibilities is there if no signature by SS. Secondly, even with the signature form SS, the given signature do not help nonce version. Due to absence of the nonce version attacker can reply with given nonce to BS, so, an interleaving attack possibilities is there.

2. Man in the middle attack:

The PKMv2 protocol provides the mutual authentication using three way handshaking, so the possibility of man in middle attack is eliminated. However this is still vulnerable to MITM attack. One the network will do initial network entry procedure it is not going to provide any security mechanism in SS and BS negotiation parameters. Protocol not implemented security in initial parameter due to fast handover support, so by capturing this parameter an attacker can register himself with false SS or BS.

3. Multiple Attack

A new type of attack introduce by author [9] in X.509 tripartite authentication protocol even with checking of timestamp, in this type of attack one factor commit mistake on the multiplicity of the meeting. The attack can be avoided by adding BS identity.

V. Conclusion

Wireless security is the big challenge for the recent trend, as discussed in this paper PKMv1 protocol is completely unsuccessful to maintain the security. However the Pkmv2 protocol overwhelms the weakness of version 1 protocol but still it is not fully endangered. As it is a great enhancement for authentication, PKMv2 introduces EAP as extra authentication process and it can be used together with RSA authentication, which is also improved by adding mandatory mutual authentication. The Pkmv2 protocol strengthens the security feature around many areas:-confidentiality, authentication but still lack behind in the area of integrity and non-repudiation during the authorization process. So Pkmv2 protocol play major role to maintain security in Wimax environments but still it's vulnerable to some threats.

References

[1]. Rajesh Srivastava, Deepak Kumar Mehto, Prevention of Security Threats in IEEE 802.16 Standards, International Journal of Soft Computing and Engineering (IJSCE) 1(4), 2011, 103-108.
[2]. Rakesh Kumar Jha, Dr Upena D Dalal, A Journey on WiMAX and its Security Issues, International Journal of Computer Science and Information Technologies, Vol. 1 (4), 2010, 256-263.
[3]. Karen Scarfone Cyrus Tibbs Matthew Sexton, Guide to Securing WiMAX Wireless Communications, Recommendations of the National Institute of Standards and Technology,(NIST Special Publication 800-127) 44 pages (September 2010).
[4]. Glen Zorn, RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol Support, Internet Engineering Task Force (IETF), Request for Comments: 590, 2010.
[5]. Sanida Omerovic, WiMax Overview, Faculty of Electrical Engineering, University of Ljubljana, Slovenia,pp.1-35.
[6]. Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski, IEEE 802.16 Security Issues: A Survey, Proc. 16th Telecommunications Forum TELFOR 2008, Belgrade, Serbia, Nov 2008,25-27.
[7]. Byeong Gi Lee, Sunghyun Choi, Broadband Wireless Access and Local Networks Mobile WiMAX and WiFi, (**US** Library of Congress Cataloguing-in-Publication Data, 2008).
[8]. Fuden Tshering, Anjali Sardana, A Review ofPrivacy and Key Management Protocol in IEEE 802.16e, International Journal of Computer Applications (0975 – 8887),Volume 20– No.2, 2011, 25-31.
[9]. X. Sen and H. Chin-Tser, "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions," Proc. in Wireless Communication Systems, 2006. ISWCS '06. 3rd International Symposium, 2006, pp. 185-189.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Rajesh Kumar Study of PKM Protocols and Threats in Wimax" IOSR Journal of Computer Engineering (IOSR-JCE) 21.3 (2019): 10-15.