Indian Journal of Science and Technology, *Vol 7(3), 282–295, March 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks

A. S. Khan[1], N. Fisal[1], Z. A. Bakar[1], N. Salawu[1,2*], W. Maqbool[1], R. Ullah[1] and H. Safdar[1]

[1]UTM-MIMOS Center of Excellence, FKE, UTM, Malaysia; adnan.ucit@gmail.com, Sheila@fke.utm.my, zurkarmawan@fke.utm.my, salawunathaniel@gmail.com, wajahat_maqbool@yahoo.com, eng.rahat.u@ieee.org, eng.hassim.s@ieee.org

[2]Telecommunication Engineering Department, Federal University of Technology, P. M. B. 65, Minna, Niger State, Nigeria

Abstract

Mobile Multihop Relay (MMR) network is one of the emerging technologies, especially LTE-Advanced, WiMAX and the Smart grid communications. Ensuring security is one of the most imperative and challenging issues in MMR networks. Privacy Key Management (PKM) protocol is proposed to ensure the security measures in MMR networks. However, the protocol still faces several security threats, specifically Denial of Service (DoS), replay attacks, Man in the Middle (MitM) attacks and the interleaving attacks, which is termed as Medium Access Control (MAC) layer attacks. This paper proposed a modified version PKM protocol for both unilateral and mutual authentication, which is termed as Self-organized Efficient Authentication and Key Management Scheme (SEAKS) authentication protocol. This protocol ensures secure end-to-end data transmission using distributed hop-by-hop authentication and localized key management schemes with a very simple and efficient way. The performance evaluation of the proposed schemes in terms of packet delivery ratio, packet overhead, processing time and the effect of increasing number of rogue relay stations is carried out and compared with the official draft of MMR WiMAX and the SEN XU. The result showed that our proposed scheme out-performed the base line protocols.

Keywords: Denial of Service, Hop-by-Hop Authentication, IEEE 802.16, MMR WiMAX Network, Security Issues

1. Introduction

Introduction of relays to support multi-hopping in MMR WiMAX networks not only increases the wireless converges but also provides features such as lower backhaul deployment cost, easy setup and high-throughput[1]. Security is essential in wireless technologies to allow rapid adoption and enhance their maturity. Security specifications can mainly be found within the MAC layer, which is called security sublayer. WiMAX has security vulnerabilities, which may create a significant disruption in communication with little effort from the attacker thus could threaten its wide-spread deployment[2]. In the security sublayer of WiMAX, two sets of protocols are provided: an encapsulation protocol for encrypting data across Broadband Wireless Access (BWA), and a PKM protocol for secure distribution of keying materials from the Base Station (BS) to the Subscriber Station (SS) and for enforcing conditional access by the BS. The PKM protocols work in two different versions, i.e. PKMv1 and PKMv2. PKMv1 allows only unilateral authentications, and PKMv2 allows mutual authentications. It also supports periodic re-authentication/re-authorization and key refresh[3]. The PKM's authentication protocol establishes a

*Author for correspondence

shared secret Authorization Key (AK) between the SS and the BS. The shared secret is then used to secure subsequent PKM exchanges of Traffic Encryption Keys (TEKs). An SS uses the PKM protocol to obtain authorization and traffic keying material from the BS and to support periodic reauthorization and key refresh. PKM supports two distinct authentication protocol mechanisms that are RSA (Ron Rivest, Adi Shamir and Leonard Adleman) protocol[1], and Extensible Authentication Protocol. This study only focuses on PKM-RSA protocol.

In general, research challenges for MMR WiMAX network arise primarily due to the large number of constraints that must be simultaneously satisfied. One of the major constraints is the lack of physical boundaries that leads towards several attacks, especially DoS, replay attack, MitM attack and interleaving attacks[4–6]. Secondly; authentication overhead is also one of the key constraints. In MMR network, either centralized authentication or distributed authentication can be used. If centralized authentication is used, every multihop node should always be accessible to the authenticator server, therefore, could be overloaded to handle the mutual authentication among all nodes on the network. Hence, each multihop node needs to contact the authentication server whenever authentication is required. This scheme may generate authentication overhead and thus is not suitable for MMR networks where each node keeps moving and wants to authenticate many neighbor's nodes[4,7,8]. On the other hand, if distributed authentication is used, it is very difficult to share initial trust information among the relays for mutual authentication. Thirdly, due to lack of trust within the participating relays, an internal attack may occur from the rogue relay stations[9–11]. If this rouge relay station increases thus cause a severe and unbearable loss to the deployment. However, author[9] discussed Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations. This protocol works better for the centralized security mechanism where the scalability is the issue. Author[3] described all the possible attacks and their countermeasure; however, they mainly focused more on mobile WiMAX, thus literature on the modification of PKM protocol for MMR networks is scare. To countermeasures such constraints, distributed hop-by-hop authentication with localized key management and re-authentication that can ensure secure end-to-end data transmission is required.

As far as we are aware of, this is the first attempt to come up with the modified version of PKM for MMR WiMAX network after the official draft 2009 released. The proposed authentication schemes work for the distributed hop-by-hop authentication which provides security as well scalability to the networks.

The remainder of this paper is organized as follows: The next section describes basic concepts of MMR WiMAX networks. Section III presents our proposed security mechanism, which is SEAKS authentication protocol. Section IV illustrated results and discussion followed by section V where we conclude.

2. Mobile Multihop Relay WiMAX Networks

In IEEE 802.16j-2009[1], multihop relays is an elective deployment to support performance and coverage area in WiMAX networks. In multihop relays network, BS can be modified to Multihop Relay-Base Station (MR-BS). Communication within SS and MR-BS are relayed through Relay Stations (RS), thus enhancing the coverage area and efficiency of the network. Multihop relays are partially or fully under the supervision of MR-BS. It thus leads towards two different modes viz. centralized and distributed scheduling modes. Relays with full MR-BS supervision is functioned under centralized scheduling mode where MR-BS is full responsible for all the decisions. Relays with partial MR-BS supervision functioned under distributed scheduling mode where all the decisions are taken by RS with the collaboration of MR-BS[7]. Relays are categories into two, non-transparent and transparent relays. Non-transparent relays function in both centralized as well as distributed scheduling mode. However, for transparent relays, it only can function in centralized scheduling mode. These relays can operate in three separate schemes depending upon the processing of received signals. These schemes includes amplify and forward, decode and forward and estimate and forward. Decode and forward and amplify and forward relay are also termed as non-transparent relays and transparent relays respectively. These relays may be fixed in location like mounting to the top of the building or mobile traveling on vehicles[11].

As far as security matters are concerns, these relays worked in two different security modes i.e. centralized security mode and distributed security mode. In this paper, we use distributed security scheme. However, centralized security scheme normally resides in MR-BS in the multihop relay system where Security Association (SA) is

established within RS and MR-BS without the participation of intermediate RS. The intermediate RS does not decrypt the user data payload or do any kind of authentication to the SS or other RS; it just relays what MR-BS transmits to it. MR-BS is responsible for managing all the keys related to SS or RS. Intermediate RS does not have any key information related to SS. In the distributed security scheme, the authentication keys established within SS and MR-BS is transferred to intermediate RS, during the registration to network, intermediate RS based on its capability may be configured to work in distributed security mode[12]. An intermediate RS operating in this scheme initiate the RSA-PKM authentication protocol within MR-BS and itself, once AK is established within these two entities; MR-BS securely transfer the relevant authorization keys of the other requesting RS/SS to this intermediate RS. This intermediate RS will derive all necessary keys and starts RSA-PKM authentication protocol with other subordinate RS/SS. After receiving the relevant keys from MR-BS intermediate RS will re-encrypt the relayed MAC PDU[1].

2.1 Security Requirements and Issues of MMR WiMAX Networks

The security sublayer lies above the physical layer and below the MAC CPS, which is encrypted, authenticated and validated. However, header and control information added by the physical layer are not encrypted or authenticated. Thus, physical layer information attached to the higher layer packets is vulnerable to threats. The MAC management messages are sent in the clear to facilitate network operations. Thus, MAC header and MAC management messages are sent unencrypted give a wide field for the attacker to play[13,14].

DoS attack on the BS may ensue when an adversary intercepts the Auth-Req (Auth-Req) message transmitted by the legitimate SS/RS and save that message. Adversary will use this message by resending it after specific period of time to perform replay attack against BS. However, the adversary may not decrypt the Authentication Response (Auth-Rsp) messages keying parameters, but it will replay this message multiple times to exhaust the capabilities of MR-BS. This may cause the denial of service to the legitimate SS. On the other hand, SS/RS also faces this type of attack even worst then the MR-BS. Adversary may develop its own Auth-Rsp message by generating AK and sent to the SS impersonating as MR-BS. Thus can gain the control over the complete communication, this is called typical Man-in-the-middle attack[15]. MR-BS authentication process in PKMv2 is vulnerable to an interleaving attack. In this attack, the attacker impersonates a valid RS, exchange the first two messages of PKMv2 sequences with a valid MR-BS, and then it replays these to the original, valid RS to gain the final PKMv2 messages. The attacker then uses the final message from the original RS to complete the original PKMv2 sequence with the MR-BS. This results in unauthorized access over the network. As the number of hops increased in the distributed and non-transparent environment, unreliability increases thus more powerful and complex attacks can be attempted.

In the case, when the attacks involve the MR-BS, it's a little tricky for the adversary to get successful as MR-BS is a much more intelligent device, however, if the case when RS in involve as RS is not too complex and intelligent, then the MR-BS, thus the chance of different attacks for RS is higher than BS[6,7,16]. MMR WiMAX networks demand such security measures that can tackle these MAC layer attacks with fewer authentications overhead and ensure secure end-to-end data transmission.

3. Proposed Security Mechanism

To address the above security issues, SEAKS is proposed. SEAKS consists of two main functional modules that include authentication management and key management. The Authentication management is incorporated with SEAKS-PKMv1, SEAKS-PKMv2, and authentication mechanism for single as well as for multihop and re-authentication mechanisms. The Key management consists of AK management and TEK management. Distributed authentication features of SEAKS protocol is illustrated in single as well as multihop authentication scheme. State machines for AK and TEK highlight the mechanism of localized key re-authentication and key management.

SEAKS is based on self-organized model using non-transparent, decode and forward relay. SEAKS provides a hybrid authentication scheme with distributed authentication and localized re-authentication and key maintenance. However, this technique not only helps in minimizing the overall authentication overhead on MR-BS and authentication server but also provides an efficient way to countermeasure the vulnerabilities. The functional components of SEAKS are shown in Figure 1. The detailed and exhaustive discussion of authentication management and key management will be discussed in section 3.1 and 3.2 respectively.

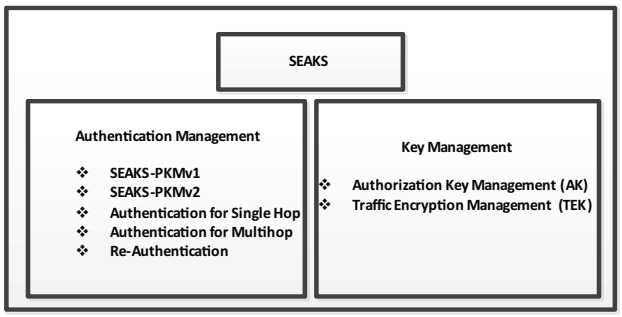

Figure 1. Functional Components of SEAKS.

3.1 Authentication Management

Authentication management allows both SEAKS-PKMv1 and SEAKS-PKMv2 authentication protocols to authenticate and to perform key exchanges between the SS/RS/N-RS and the MR-BS using client server mode. SEAKS authentication management provides a self organized and cost efficient mechanism for multiple N-RS to authenticate itself in distributed and hop-by-hop security control and also allows re-authentication in localized security controls.

In any security matter, two distinct functions must be considered carefully, i.e. authentication and secrecy. Often, authentication is needed but not secrecy and vice versa. PKM protocols utilize three messages to get N-RS authenticated with MR-BS. The first two messages are Auth-Info and Auth-Req, while the third message is Auth-Reply as shown in Figure 2. Since the first message is highly informative and optional, analysis will be carried out from message 2. Message 2 is always sent in a plain text as capabilities and Security Association Identifier (SAID) is already shared between MR-BS and N-RS during Subscriber Basic Capabilities (SBC) and ranging process. Secondly, certificates must be sent in a plain text as a public key cannot be accessed by MR-BS. Message 2 is also highly vulnerable to all sorts of attacks. In this case, only the authenticity of the message is required not the secrecy. The key goal is to transmit the message in such a way that "*attacker cannot alter or modify the message*." Thus, helps in avoiding replay, DoS and MitM attacks. Similarly, message 3 also exposes the SS to replay attacks even worst. To avoid the replay attacks in message 3, both authenticity and secrecy are required, which includes, "*message should not be modified and should come from the legitimate MR-BS*".

3.1.1 SEAKS-PKMv1 Authentication Protocols

In this section, we will elaborate the authentication steps of our proposed authentication protocol. SEAKS can be further divided into SEAKS-PKMv1 for unilateral authentication and SEAKS- PKMv2 for mutual authentication. In SEAKS- PKMv1 a node SS/N-RS begins the authentication by sending an Auth-Info message as shown in Figure 2. Later, SS/N-RS sends an Auth-Req message to N-RS or MR-BS. The Auth-Req message contains security credentials in plaintext P. A message digest is created by hashing P with the hash function H, i.e. P (H). The Auth-Req message is generated by encrypting the message digest and the plaintext P using private key (Pri) of the sending N-RS. The encrypted Auth-Req message is represented as $\left[P \mid H(P)\right]_{N-RS_{Pri}}$.

MR-BS receives the Auth-Req and decrypts it using the sender's public key. The receiving node N-RS or MR-BS will hash the received plaintext P and then compare with the received message digest. If both values are exactly the same, the Auth-Req message is valid and the originality of the message is authentic. Once the authenticity of the Auth-Req message is validated, N-RS or MR-BS will generate an AK and prepare an Auth-Rsp message. Auth-Rsp message is generated differently from Auth-Req message in order to maintain secrecy as well as authenticity. First, N-RS or MR-BS encrypts all the security credentials, including AK with its private key to ensure secrecy. The encrypted information is Pri (security credential) is defined as Q. Next, N-RS or MR-BS will compute the message digest H (Q) by hashing Q. Finally, both Q and the message digest will be encrypted using N-RS or MR-BS private key to form Auth-Rsp message. The encrypted Auth-Rsp message can be represented as $\left[Q \mid H(Q)\right]_{MR-BS_{Pri}}$. SS/N-RS receives the Auth-Rsp message and decrypt it using sending SS/N-RS or MR-BS public key. The receiving node will hash the received Q and then compare with the received message digest. If both values are exactly the same, the Auth-Req message is genuine and thus the originality of the message is authentic.

The main purpose of replay attack is to replay the message several times (hit and trial) to either exhaust the N-RS/MR-BS sever (DoS attack) or to get control of the communication link (MitM attack). In this paper, the major intention of the replay attack is to get the control of the communication link. For the successful MitM attack, an adversary must modify the authentication message. The proposed protocol prevents replay attacks at the SS/N-RS or MR-BS and hence overcomes the MAC layer attacks. SEAKS- PKMv1 ensures the transfers of Auth-Req and Auth-Rsp messages with authenticity, non-repudiation and secrecy. In MMR with SEAKS, if any adversaries try

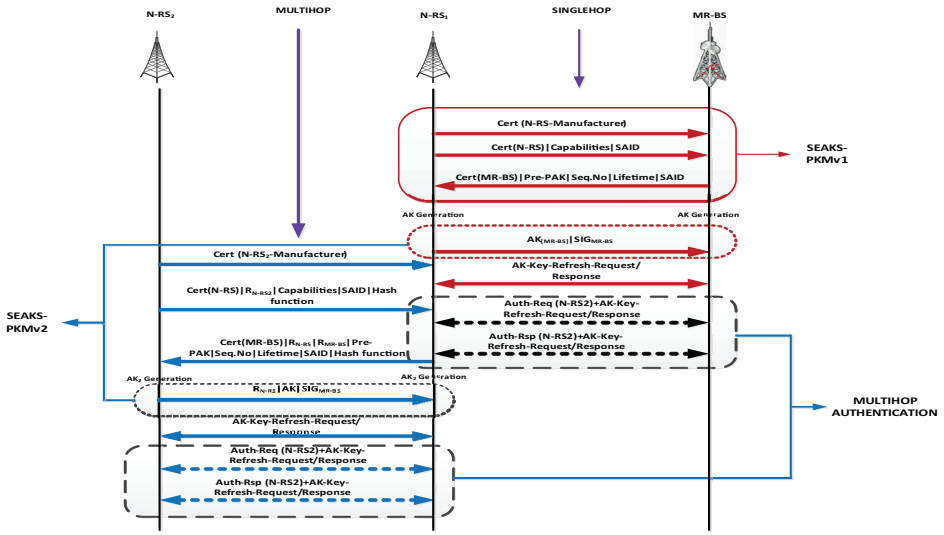

Figure 2. SEAKS Authentication Protocol.

to intercept Auth-Req or Auth-Rsp message, they cannot modify a single bit of the message due to hash function, consequently; they cannot generate replay attacks. In case, any modification is found, N-RS or MR-BS silently discards the message. However, if the adversary replays the message without modification (a case of simple amplify and forward), MR-BS facilitates the message and sends the response to the legitimate user as the certificate belongs to the legitimate user.

3.1.2 SEAKS-PKMv2 Authentication Protocols

Due to lack of mutual authentication in PKMv1, the IEEE 802.16 standard has proposed PKMv2 in which one additional message is added at the end of the original authentication protocol of PKMv1. However, PKMV2 belongs to the three-way authentication[1] with a confirmation message from the SS to the BS. Since the first message is optional and only informative, the security analysis began from the next message. Message 2 is sent without the signature. Without the signature of the SS, the request message is easily modified or impersonated. This is similar to what was discussed in PKMv1 and again this is referred to as simply replay attack that can also result in DoS. Due to the lack of signature in message 2, impersonation is not a problem, which leads to the interleaving attack[19]. Interleaving attack arises if an attacker can modify the message 2, sent by the MR-BS to the legitimate N-RS by replacing the Cert MR-BS and SIG MR-BS with Cert (Attacker) and SIG (Attacker), respectively. Even with signature from N-RS serving as message authentication, interleaving attack can still occur. SEAKS-PKMv2 authentication protocols help to resolve the above-mentioned threats in an efficient manner. SEAKS-PKMv2 is basically forward and backward compatible and work with both IEEE 802.16e in distributed and non-transparent relay based IEEE 802.16 network. The protocol is well explained in Figure 2.

In Auth-Req message, instead of using signatures or using public key cryptography, SEAKS-PKMv2 protocol uses a hash function that not only helps in avoiding a replay attack, but also helps to counter interleaving attacks. Adding hash function in message 3 also helps in avoiding impersonation. Modification of message can be easily identified, and the whole message will be silently discarded by the MR-BS. As far as an acknowledgement message for MR-BS response message is concern, only AK encrypted by the public key of MR-BS with random number is transmitted to MR-BS. This is to ensure the authenticity, non-repudiation and secrecy of this message.

The authentication mechanism residing at N-RS is responsible for getting AK and valid list of SAIDS. N-RS is also responsible for authenticating itself with MR-BS and the neighboring N-RS. The state machine diagram for SEAKS authentication management is shown in Figure 3. The SEAKS authentication state machine also gives birth to not only AK and Re-Auth, but also TEK refreshment. The state machine for SEAKS consists of 9 states and 9 distinct events. The nine states include Start, Auth-Wait,

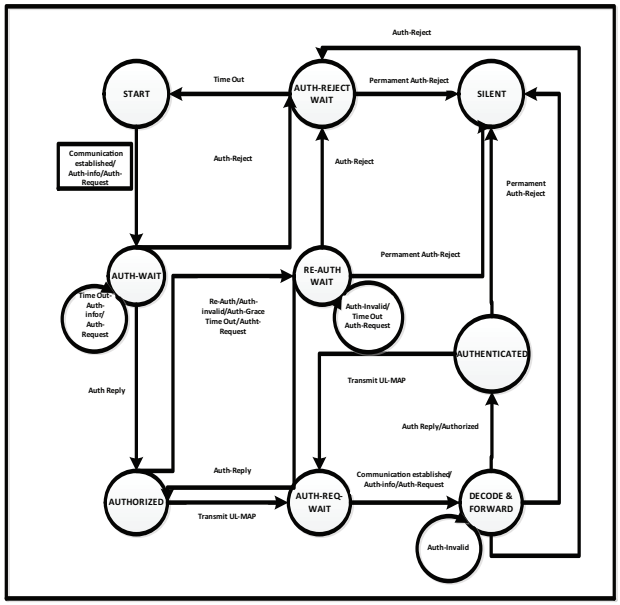

Figure 3. SEAKS authentication state machine.

Authorized, Auth-Reject-Wait, Re-Auth-Wait, Re-Req-Wait, Silent, Decode and Forward and Authenticated. The nine events include communication established, Timeout, Transmit UL-MAP, Auth-Grace-Time Out, Auth-Key-Authorized, Perm-Auth-Reject, Auth-Reject, Re-Auth and Auth-Invalid.

The state diagram illustrates the protocol messages' transmitted and internal events generated for each of the models state transitions; however, the diagram does not indicate additional internal actions, such as clearing or starting of timers that accompany the specific state transitions. SEAKS begins in the "Start" state; an initial state where no resources are allocated or used. A communication is established upon entering the start state, if the MAC has completed the basic capability negotiation. Once the communication is established, N-RS is now eligible to send Auth-info and Auth-Req message to MR-BS to obtain AK and the list of authorized SAIDs. The second state is Auth-Wait, where after sending authentication information and Auth-Req message to MR-BS, N-RS waits for the response.

If N-RS received an Auth-Reply message that contains the lists of valid SAIDs and AK, it moves to the authorized state. Otherwise, it will stay at Auth-Wait state and wait for the Auth-replay. At Auth-wait state, if the time out occurs and Auth-replay is not received; it moves to Auth-reject phase. However, at Auth-reject wait, if time out occurs, authentication procedures will start from the scratch, and it moves to start state. If MR-BS sent permanent Auth-reject at Auth-reject wait state, it moves to silent state. Once N-RS is authorized, it starts transmitting UL-MAP and move to Auth-Req-wait. If it received Auth-info or Auth-request message, if moves to decode and forward state. In this state, if Auth-Req is invalid, it will remain in this state. Otherwise, it authenticates the requesting N-RS. At decode and forward state, if Auth-rejection occurs, it moves to Auth-reject wait, or if it receives a permanent rejection from serving N-RS, it moves to a silent state. Once authenticated, the newly joined N-RS starts transmitting UL-MAP and waiting in the Auth-Req message from any other N-RS.

3.1.3 Authentication Procedures for Single Hop

To understand the authentication procedures for single hop in MMR WiMAX network, consider an $N\text{-}RS_1$, who wants to join the WiMAX networks. $N\text{-}RS_1$ sends its Auth-Req message to the serving MR-BS. In response to an authorization request message, an MR-BS validates the requesting N-RS's identity, determines the encryption algorithm and protocol support, activates an AK for $N\text{-}RS_1$, encrypts it with the $N\text{-}RS_1$'s public key and sends it back to the $N\text{-}RS_1$ in authentication response message.

It also includes 4 bit sequence number, used to distinguish between successive generations of AKs, a life time, and the securities' identities for which $N\text{-}RS_1$ is authorized to obtain keying parameters. Once authenticated and the Authorization Key (AK) is obtained, $N\text{-}RS_1$ must periodically refresh its AK by reissuing an Auth-Req message to the MR-BS. During the reauthorization cycle, to avoid service interruption, AKs have overlapping lifetime. Both N-RS and MR-BS support up to two simultaneously active AKs during this transition period. Authentication of $N\text{-}RS_1$ with MR-BS is shown in Figure 4. Once $N\text{-}RS_1$ achieves authorization, it starts a separate TEK for each SAID defined in the authentication response message.

3.1.4 Authentication Procedure for Multihop

Figure 5 illustrates the authentication procedure for multihop networks. Consider a second $N\text{-}RS_2$ that wants to join the network. Due to its non-transparent nature, it is not in the coverage of MR-BS and only $N\text{-}RS_1$ can listen to it. In this case, $N\text{-}RS_2$ listened to the UL-MAP from $N\text{-}RS_1$ and sends the Auth-Req message to $N\text{-}RS_1$. However, any non-transparent node that wants to join the network must have to authenticate itself with MR-BS, as MR-BS is

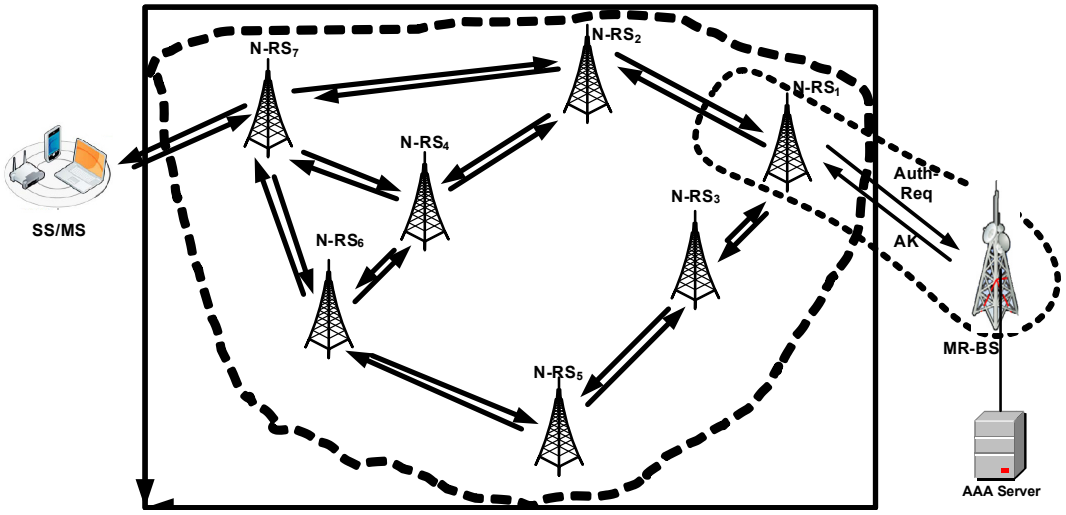

Figure 4. Authentication of N-RS$_1$ with MR-BS.

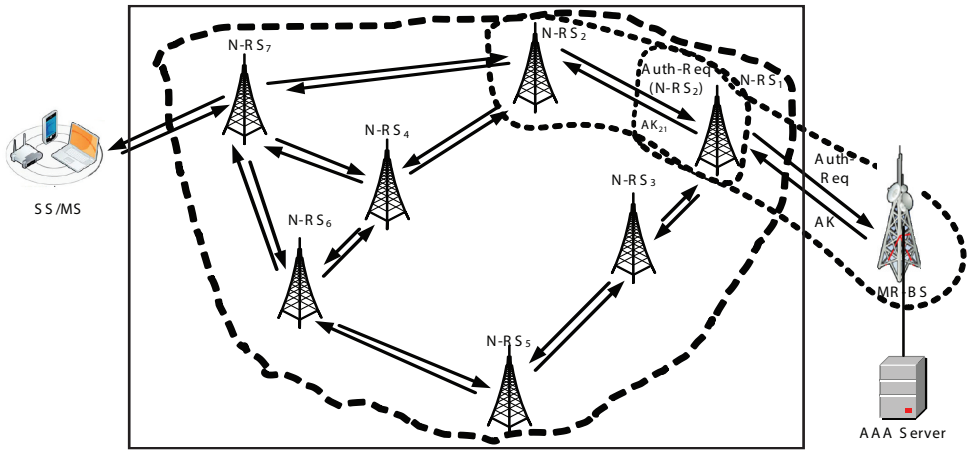

Figure 5. Authentication of N-RS$_2$ with N-RS/MR-BS.

directly attached to the authentication server. Meanwhile, N-RS$_1$ cannot authenticate N-RS$_2$ on behalf of MR-BS. According to SEAKS, N-RS$_1$ received the Auth-Req message from N-RS$_2$ and sends it to MR-BS during the refreshing of AK message. N-RS$_1$ receives MACPDU of N-RS$_2$ and encapsulates it into its own PKM-REQ message of type 9 and codes 4 [1].

According to Figure 5, MR-BS receives MAC-PDU of N-RS$_1$, which is basically sent for refreshing AK. MR-BS will check MAC header of N-RS$_1$. If RAR (Relay Auth Request) is equal to 1, it means that there is one relay request inside MAC-PDU. RAR is basically the reserve bit utilized for RAR indications. Once MR-BS obtains Auth-Req of N-RS$_2$, it validates its authenticity and activates AK$_2$ and other parameters, encrypts it with N-RS$_1$ public key and responds to N-RS$_1$ in its Auth-Rsp message. N-RS$_1$ receives N-RS$_2$'s security information, saves one copy of all information into its table, generates AK$_{21}$, encrypts it with N-RS$_2$ public key, and sends it Auth-Rsp message to N-RS$_2$. Once N-RS$_2$ is authenticated, it will initiate separate authorization and traffic encryption key with N-RS$_1$.

3.1.5 *Re-Authentication and Self-Organized MMR Networks*

All N-RSs maintain knowledge shared table of recently exchanged AK with its neighbors. If N-RS$_2$ fails to

re-authenticate before the expiration of its current AK, N-RS$_1$ will wait until it sends Auth-Req message. If N-RS$_2$ sends the Auth-Req message again, rather than sending this request to MR-BS, N-RS$_1$ will check its own table. If N-RS$_2$'s certificate is found within its table, it will validate N-RS$_2$ authenticity locally. Thus enhance the communication cost efficiency in terms of authentication overhead, which lessens the overall complexity of the protocol. Figure 6 shows the authentication mechanism of more than two N-RS with MR-BS. In this case, if N-RS$_3$ wants to join the network, it will send the Auth-Req message to N-RS$_2$, as it is working in non-transparent mode. While sending the message, N-RS$_3$ will set RAR=1 inside the MAC header so that N-RS$_2$ can recognize that there is one Auth-Req message inside the Mac payload, and set the TYPE value =8 and code =4, which means it is PKM-AUTH–REQ message. Once N-RS$_2$ receives this message, it will check RAR values. If the value is one, it will save the message to its table, and forward it to N-RS$_1$. Before sending, it will again set the RAR=1.

Hence, there are two MAC messages present inside the MAC payload of N-RS$_2$, one is Auth-Req (code 4) and the other is Key-Req (code 5). N-RS$_1$ will receive this message and check RAR value; if it is 1 then it will copy the Auth-Req message to its table, otherwise it will ignore and forward it to MR-BS. MR-BS will receive the message and validate it. MR-BS will send back the Auth-Rsp message with type 9. Again here, there are two MAC messages inside the MAC payload, one is with Key Reply (code 8), and the other is Auth-Reply (code 5) to N-RS$_1$. N-RS$_1$ checks the code values, if it is 5, it will send to N-RS$_2$. If 8, then it will use for its refreshing of keys. N-RS$_2$ again receives two MAC messages inside the payload; one is with code 5, and the other is with code 8. It will retain code 8 with itself and send the code 5 message to N-RS$_3$. Thus, N-RS$_3$ is authenticated with MR-BS with distributed manner and maintains its keys locally as mentioned in the previous sections. Likewise, if any other N-RS such as N-RS$_4$ and N-RS$_5$ want to join the network, they will follow the same procedures. After a specific interval of time, all the N-RSs shared their knowledge tables thus creating a self-organized environment. This self-organized environment is responsible for distributed authentication and localized re-authentication and key management.

3.2 Key Management

In MMR networks, SEAKS allowed multiple N-RSs to participate for coverage and throughput enhancement. Once the authentication process is completed and all the participating devices are registered to the MR-BS, the AK shared need to be refreshed periodically. This refreshes initiate by reissuing an Auth-Request message to the MR-BS. Re-Auth is identical to authentication with the exception that the N-RS does not send Auth. Info message during Re-Auth cycles. To avoid service interruption during Re-Auth, successive generations of the N-RS's AK have overlapping lifetimes. Both N-RS and MR-BS are able to support up

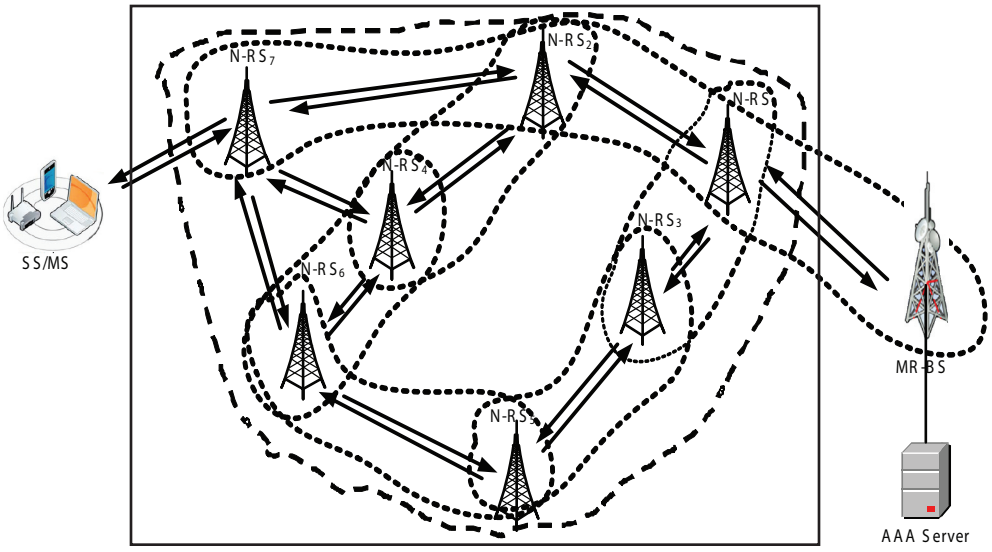

Figure 6. Authentication of N-RS$_n$ with N-RS$_1$/MR-BS.

to four and two respectively and simultaneously active AK during their transition periods[17].

3.2.1 Authorization Key and Re-authentication Management

The proposed SEAKS protocol supports participating devices to refresh AK periodically and to re-authenticate locally if necessary. The state machine diagram for SEAKS AK and Re-authentication mechanism is well illustrated in Figure 7. AK and Re-Auth refreshment state machines consist of six states, which are started, authorized, operation wait, operation Re-key wait, and Re-Auth. It has five events, which are key pending, key reject, key Grace time out and key life time. In the initial stage, no resources are assigned. All the timers are off, and no processing is scheduled. From the start state, it is assumed that N-RS successfully obtained the AK and valid lists of SAID, thus it moved to authorized state. At this state, N-RS needs to send the key request and obtain the key response messages in order to refresh AK periodically.

Once the key request has been sent, N-RS moved to operation wait state and wait for the key replay. If it receives the key replay from MR-BS, it moves to operation state. Operation state is the stable state where N-RS has the valid and refreshed AK. During the operation state, if the lifetime of AK is near to expire, N-RS moves to rekey-wait state by sending the key-request. If the key request appears to be invalid, N-RS moves to authorized state, where it needs to send the key request again. Otherwise, it receives the refreshed AK and moved to operation state. During the operation state, if the key request is not sent and the key grace time exceeded its limit; N-RS moves to Re-Auth state. During the Rekey-wait, if the key request is rejected, it moves to Re-auth state. It also moves to Re-auth state during the authorized state when the key request grace time exceeded, and N-RS does not receive any key replay message from MR-BS. During Re-auth state, it sends the Auth-Req to MR-BS, and MR-BS is always ready to restart re-authentication upon request.

3.2.2 Traffic Encryption Key Management

Once authenticated and sharing of AK has been successfully completed, N-RS initiates a separate TEK for each of the SAIDs indentified in the Auth-Reply message. Each TEK operating within the NRS is responsible for managing the keying parameters associated with its respective SAID. Communication between authorization state machine and TEK state machine is done through triggering the events or protocols. However, if the authorization state machine[1] receives authentication reject message from MR-BS, it will stop all of its TEK state machines. The SEAKS TEK state machine is well illustrated in Figure 8.

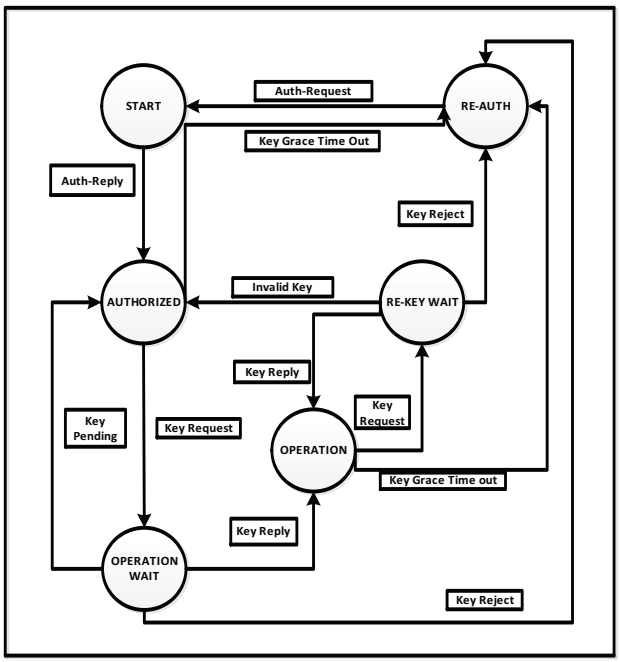

Figure 7. SEAKS AK and Re-auth mechanisms.

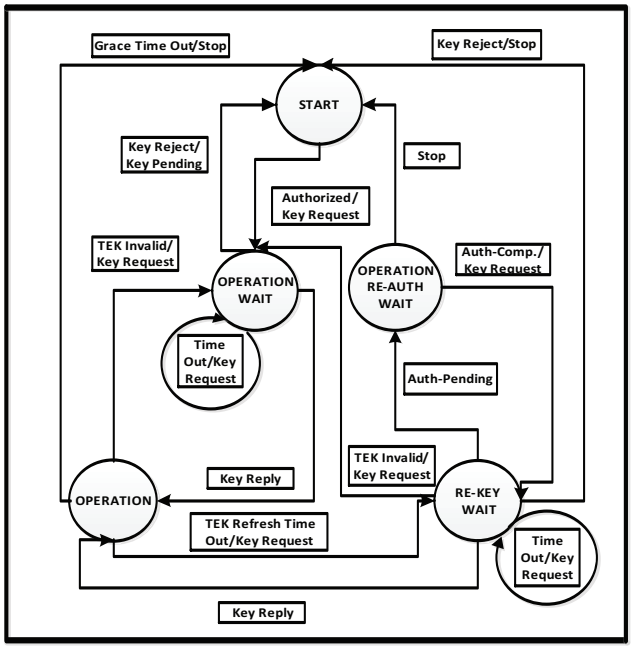

Figure 8. Traffic encryption key mechanisms.

In the TEK state machines, Key-Request message is periodically sent to the MR-BS, requesting a refresh of keying material for their respective SAIDs. MR-BS responds by sending a Key-Reply message, containing the MR-BS active keying material for the specific SAID. The TEK state machine consists of five states, which are Start, Operation wait, Operation, Operation Re-Auth-Wait and Key-Wait, and eleven events, which are Key-Request, Key-Reply, Key-Reject, TEK Invalid, Stop, Authorized, Auth-pending, Auth-complete, Time Out, TEK Refresh time out, and Grace Time Out.

All the times and processing are off during the start state. In the operational wait state, it is assumed that N-RS is authorized and sends the key request message for its corresponding SAIDs and waits for the replay. During this state, if the key request is rejected or still pending, it will proceed to start state. However, if it receives the key replay, it moves to operation state, otherwise it will send the key request again. Once the time is out, operation state is the stable state when N-RS has valid keying parameters corresponding to its SAID lists. During the operation state, N-RS sends the key request to refresh the TEK and proceeds to Re-key wait state. However, if the grace time out occurs and N-RS cannot send the key request, it will move to state again. During the Rekey wait state, if N-RS receives key replay successfully, it will move to operation state. However, during Re-key wait, if the key request sent is invalid, it will move to operation wait by sending the key request again. Otherwise, if the key is rejected, it moves into the start state. During Re-key wait, if any authentication is pending, it will move to operation re-auth wait unless until the authentication is complete or key request is sent; it proceeds to Re-key wait state again. Otherwise, if re-authentication is stopped, it moves into the start state again. Thus, the above key management and re-authentication makes the scheme self-organized.

4. Results and Discussion

The network model for MMR network security has been developed based upon the parameters mentioned in Table 1. The network model used in this research conforms to IEEE 802.16 MAC layer. Point to a Multipoint traffic pattern is used. In the simulation work, seven non-transparent relay stations are used. All the relays are associated with at least one subscriber station. Relay 7 is used as an adversary who can generate replay attack, as replay attacks are the key causes of either DoS or MitM attack or interleaving attacks. AK and TEK lifetime is set to 5s and 3s respectively. The simulation utilized RSA protocol for authentication, RSA-SHA-1 for digital signature and X.509 version 3 for digital certificates. However, the complete lists of network parameters are mentioned in Table 1.

The proposed security measure in distributed and N-RS-based IEEE 802.16 networks have been studied using discrete even simulator NCTUns 6.0 [18]. In the simulation study; the proposed SEAKS protocol has been implemented on the existing IEEE 802.16j topology network. The performance study of SEAKS protocols on the network simulator has been directed to study the effect of packet delivery ratio, packet overhead, processing time, effects of increasing number of compromised relay stations and effects of increasing number of Hops. Two simulations were carried out for each analysis, i.e. with or without the presence of attackers. These attackers are only responsible for replay attack as replay attacks are the key causes of all other attacks. For each simulation, three different authentication protocols were analyzed and tested: OD-2009, SEN XU and SEAKS.

Table 1. Network Parameters

Parameters	Values
AK Lifetime	5s
TEK Lifetime	3s
Authorize Wait Timeout	2s
Re-authorize Wait Timeout	2s
Authorization Grace Time	6s
Operational Wait Timeout	1s
Rekey Wait Timeout	1s
TEK Grace Time	6s
Authorize Reject Wait Timeout	10s
SA Challenge Timer	0.5s
SA TEK Timer	0.1s
Simulation Time	80s
MAC	802.16
No. Of Relay Stations	7
Adversary Type	Reply Attack
Authentication Protocol Mechanism	RSA Protocol
Key Derivation Algorithm	Dot16KDF
Digital Signature	RSA-SHA-1
Certificate Type	X.509 Version 3

4.1 Packet Delivery Ratio

The packet delivery ratio is defined as the ratio of the packet successfully arrived at the destination, and the total packet transmitted. Figure 9(a) shows the effects of packet delivery ratio in the absence of the adversary. The graph illustrates that proposed SEAK protocol experience lesser packet delivery ratio by 15.5% and 20% as compared to SEN XU and OD-2009 respectively. This is due to the reason that SEAKS protocol requires some additional processing delay to implement the security mechanism. This delay affects the packet deadline that leads to the data packets missing the end-to-end deadline.

However, Figure 9(b) shows that SEAKS protocol exhibits the higher packet delivery ratio by 13% and 22% as compared to SEN XU and OD-2009 respectively, when the attack exists. This is due to the reason that SEN XU and OD-2009 cannot defend against the replay attack properly as discussed previously.

4.2 Packet Overhead

Packet overhead is defined as the total packet sent over the network per packet received. The simulation results in Figure 10(a) show that the packet overhead of the proposed authentication scheme is very high, i.e. 28% higher than OD-2009 and 8% higher than SEN XU when there is no attack. This is only due to the proposed authentication scheme processes only legal packets and silently drops ambiguous packets, which result in slightly more packet overhead to confirm the authenticity of the received packets. On the other hand, simulation results in Figure 10(b) show that proposed SEAKS authentication scheme experience lesser packet overhead with 9% than SEN XU and 12% than OD-2009 when an adversary introduces replay attack in the network deployment. This is only due to the reasons that non-transparent relay stations do not trust the packet coming from the adversary unless until the Hashes of both plain texts matched as discussed earlier. Thus, no legal packet dropping occurs within the entire deployments. This means that the probability of received packet increases and thus packet overhead will be decreasing. On the other hand, SEN XU and OD-2009 trust the packet that came from an adversary impersonating MR-BS and SS. This means that the probability of received packets decreases thus the packet overhead increased.

4.3 Processing Time

The processing time per hop is an important parameter as it will affect the performance of the delivery ratio. The simulation results of processing time (in ms) versus the number of hops between the sender, and the receiver is plotted in Figure 11. The result illustrates that processing time for SEAKS protocol is much lesser than SEN XU and OD-2009, which is 43% and 14% respectively. The main reason is the simplicity of the SEAKS protocol to defend against any attack. Hashing function and message digest scheme are the most light-weight schemes than any other digital signature schemes, especially public key cryptography[19]. Increasing processing or executing time means that the duty cycle of microcontroller increases, which no doubt decreases the performance of non-transparent and distributed network. There is a slight curve

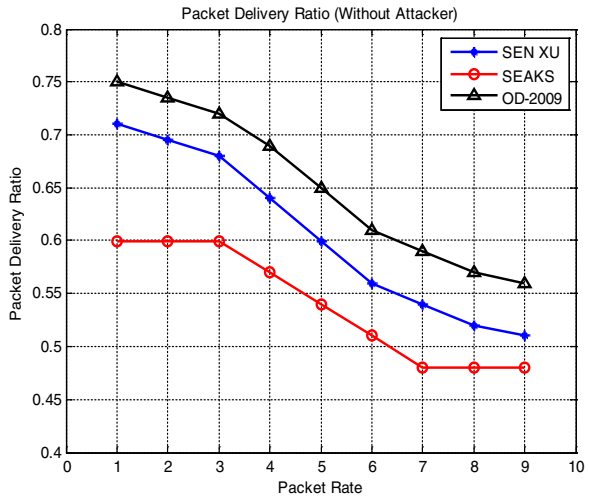

Figure 9(a). Packet delivery ratio without Attacker.

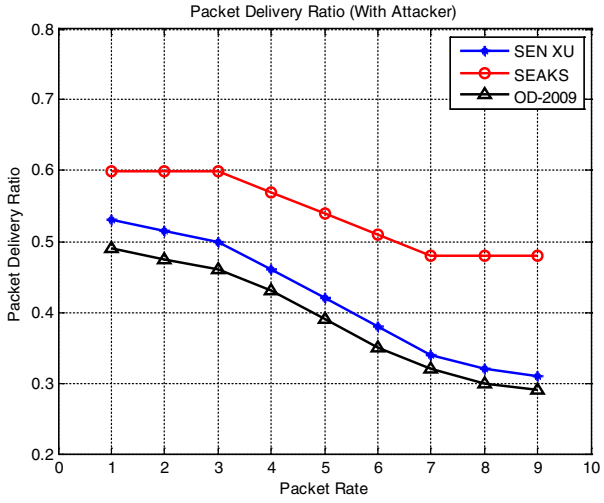

Figure 9(b). Packet delivery ratio with attacker.

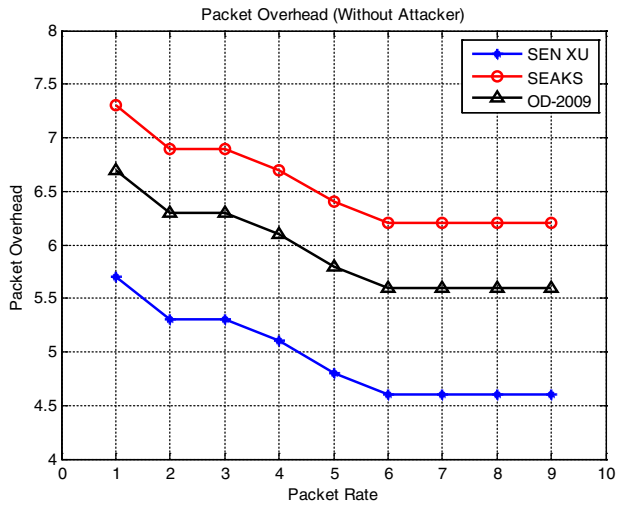

Figure 10(a). Packet overhead without attacker.

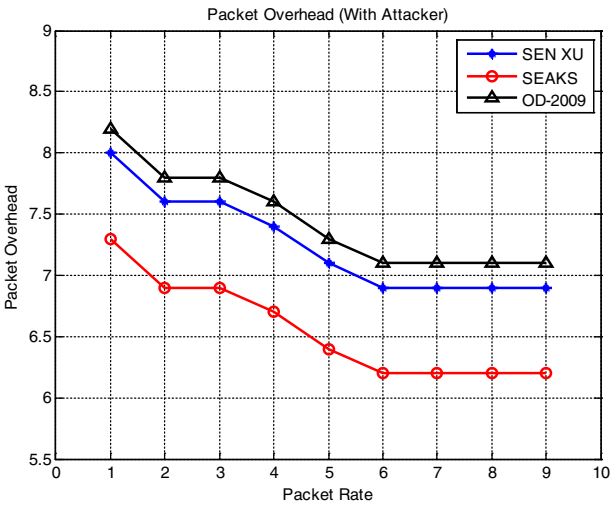

Figure 10(b). Packet overhead with attacker.

shown on the graph, after which the line gains stability that indeed shows the self-organized nature of network. Secondly, authentication is distributed and key management is localized, thus reduced the processing time once all the keys are distributed. Contrary to this, the other two authentication schemes experience high processing time. The graphs show that if the number of hops increases, the processing time increases. This is only due to the lack of self organized, distributed authentications and localized key management.

4.4 Increasing Number of Rogue Relay Stations

Rogue relay station becomes an insider attacker to allow malicious code to run inside the rogue relays. In this

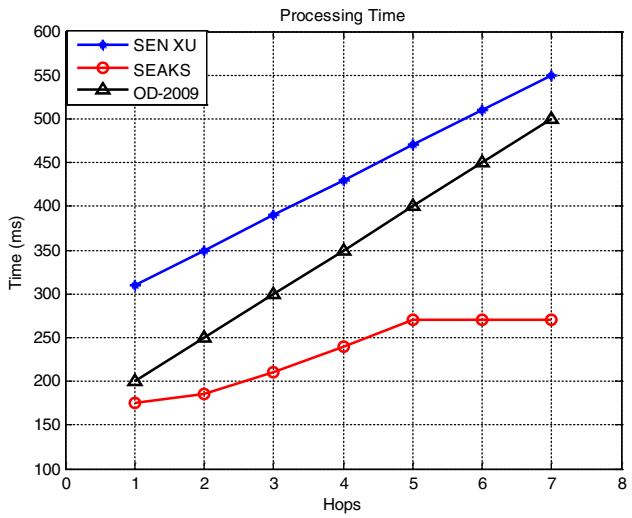

Figure 11. Comparison of processing time.

simulation study, the packet ratio is fixed, while the number of rogue relay stations is increased gradually from 1 to 7. Figure 11 shows the performance of SEAKS as compared to OD-2009 and SEN XU authentication protocols. It can be seen that the proposed SEAKS protocol exhibits the higher delivery ratio by 36% and 16% as compared to SEN XU and OD-2009 respectively. This is due to the reason that SEAKS protocol always processed legal packets (i.e. when both hash agree) and silently discard ambiguous packets (i.e. when both hash disagree). The proposed scheme shows a slight decrease in the packet delivery ratio when 5th rogue relay station is injected into the network. This is due to the processing delay that leads to the data packet missing the end-to-end deadline which affects the packet delivery ratio. On the other hand, sustainability until the injection of 4th rogue relay station is due to its self-organized, localized key management and re-authentication nature. However, the baseline authentication schemes exhibit a sharp slump until 4th rogue relay station, which is due to the reason that they trust the packets coming from the adversaries.

5. Conclusion

This paper addressed a Self-organized Efficient Authentication and Key management Scheme (SEAKS) for hop-by-hop authentication and key management scheme in non-transparent Relay-based WiMAX network. This scheme is suitable for both fixed as well as mobile non-transparent Relays. SEAKS provides the hybrid authentication scheme with distributed authentication and localized re-authentication and key maintenance.

However, this technique not only helps in minimizing the overall authentication overhead on MR-BS and authentication server but also provides an efficient way to countermeasure the vulnerabilities. Two modified PKM authentication protocols have been developed; one for unilateral authentication which is SEAKS-PKMv1 and the other for mutual authentication, which is SEAKS-PKMv2. This two authentication protocols are responsible for MR-BS and N-RSs to successfully authenticate each other and securely transfer the AK in a distributed manner. Once authentication is completed successfully and the N-RS are registered with the network, N-RS starts a separate Traffic Encryption Key (TEK) for each security identifiers (SAIDs) which is identified in the authorization reply messages from MR-BS. Traffic encryption key management is responsible for maintaining and refreshing of keys mechanism within N-RS and MR-BS. N-RS usually sent the key refresh request to MR-BS periodically and to avoid service interrupt and unwanted re-authentication; MR-BS maintains two sets of keying materials per SAID. SEAKS protocol enhances the previous works[1,6] in order to achieve high delivery ratio, minimum packet overhead and processing time. SEAKS protocol improves processing time and shows the high packet delivery ratio when rogue relay station increases. SEAKS can be employed to any MMR networks, especially LTE-A and smart grid communications.

6. Acknowledgement

The work described in this article is funded by the Research Management Center, Universiti Teknologi Malaysia (UTM.J.02.02/12.23/1/3/1 Jld.4 (16)).

7. References

1. IEEE Standard for local and metropolitan area networks part 16: Air interface for broadband wireless access systems amendment 1: Multihop relay specification, IEEE Std 802.16j-2009 (Amendment to IEEE Std 802.16-2009). 2009; 1–290.
2. Khan AS, Fisal N, Kamilah S, Abbas M. Efficient distributed authentication key scheme for multi-hop relay in ieee 802.16j networks. Int J Eng Sci Tech. 2010; 2(6): 2192–99.
3. Kolias C, Kambourakis G, Gritzalis S. Attacks and countermeasures on 802.16: analysis and assessment. IEEE Communications Surveys & Tutorials, IEEE. 2012; 15(1):487–514.
4. Mohamed El-Amin A, El-agooz S, Shehata AE-DR, Amer EA-E. Design, verification and implementation of enhanced PKM WiMAX authentication protocol. International Journal of Computer Science and Telecommunications. 2013 Mar; 4(3):41–6.
5. Altaf A, Sirhindi R, Ahmed A. A novel approach against DoS attacks in WiMAX authentication using visual cryptography. Second International Conference on Systems and Technologies in Emerging Security Information, 2008. SECURWARE '08; 2008 Aug 25–31; Cap Esterel. p. 238–42.
6. Huang C-T, Chang JM. Responding to security issues in WiMAX networks. IT Professional. 2008; 10(5):15–21.
7. Dai X, Xie X. Analysis and research of security mechanism in IEEE 802.16j. 2010 International Conference on Anti-Counterfeiting, Security and Identification; 2010 Jul 18–20; Chengdu. p. 33–6.
8. Hussain S, Khan MN, Ibrahim M. Design of distrsecurity architecture for multihop WiMAX network. Int J Comput Appl Tech. 2012; 50(9):35–9.
9. Jie H, Chin-Tser H. Secure mutual authentication protocols for mobile multi-hop relay WiMAX networks against rogue base/relay stations. IEEE International Conference on Communications (ICC). 2011 Jun 5–9; Kyoto. p. 1–5.
10. Khan AS, Fisal N, Ma'arof NNMI, Khalifa FEI, Abbas M. Security issues and modified version of PKM protocol in non-transparent multihop relay in IEEE 802.16j networks. International Review on Computers and Software. 2011; 6(1):104–9.
11. Kumar DS, Nagarajan N. Relay technologies and technical issues in IEEE 802.16j Mobile Multi-hop Relay (MMR) networks. Journal of Network and Computer Applications. 2012; 36(1):91–102.
12. Yang F, Qian Y. Two different schemes of authentication in IEEE 802.16j multi-hop relay network. 2012 8th International Conference on Networking and Mobile Computing in Wireless Communications (WiCOM), 2012 Sep 21–23, Shanghai. p. 1–4.
13. Xu S. Security protocol in WirelessMAN [Doctoral Dissertation]. University of South Carolina; 2008.
14. Sen X, Chin-Tser H, Matthews MM. Modeling and analysis of IEEE 802.16 PKM Protocols using CasperFDR. IEEE International Symposium on Wireless Communication Systems. 2008. ISWCS '08; 2008 Oct 21–24; Reykjavik. p. 653–57.
15. Ngoc NT, Maode M. An pre-authentication protocol with symmetric keys for secure handover in mobile WiMAX networks. 2012 IEEE International Conference on Communications (ICC); 2012 Jun 10–15; Ottawa: ON. p. 863–67.
16. Chee J, Ming T. Improving security in the IEEE 802.16 standards. Information Technology. 2011 Eighth International

Conference on New Generations (ITNG); 2011 Apr 11–13; Las Vegas: NV. p. 408–12.
17. Kahya N, Ghoualmi N, Lafourcade P. Key management protocol in WIMAX revisited. Advances in Computer Science, Engineering & Applications. 2012; 167:853–62.
18. Wang S-Y, Chou C-L, Lin C-C. The GUI user manual for the NCTUns 6.0, network simulator and emulator. Network and System Laboratory, Taiwan; 2009.
19. Tanenbaum AS. Computer Networks. 4th ed., Prentice Hall, PTR; 2003.