International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

# Enhancing Network Security through Advanced Authentication and Key Management Mechanisms

**Annu[1], Dr. Anil Duddy[2], Dr. Nidhi[3]**
[1] Phd Scholar, Electronics and Communication Engineering, Baba Mastnath University, Rohtak (Haryana), India.
[2] Associate Professor, Electronics and Communication Engineering, Baba Mastnath University, Rohtak (Haryana), India.
[3] Assistant Professor, C.R.A. College, Sonipat (Haryana), India.

**ABSTRACT:** This paper introduces the SEAKS-PKMv2 protocol, a robust security mechanism aimed at addressing vulnerabilities within the PKMv2 framework, particularly focusing on mutual authentication, key management, and encryption in mobile WiMAX networks. By integrating RSA-based and EAP-based authentication methods, SEAKS-PKMv2 establishes a secure environment that mitigates risks such as replay, man-in-the-middle and interleaving attacks. The protocol adopts a distributed authentication and localized key management approach, facilitating efficient and secure network access and data transmission. Through simulation, we evaluate the SEAKS-PKMv2 protocol's performance in terms of packet delivery ratio, overhead, processing time, and resilience against rogue relay station attacks. The findings demonstrate significant improvements in network security and efficiency, confirming the effectiveness of SEAKS-PKMv2 in enhancing the integrity and confidentiality of communications in distributed network settings.

**KEYWORDS:** Authentication, EAP, Encryption, Mobile WiMAX Networks, Mutual Authentication, Network Security, Key Management, RSA, SEAKS-PKMv2.

## INTRODUCTION

### Overview of Pkmv2 Protocol

The v2 protocol provides RSA-based authentication in addition to EAP (Extensible Authentication Protocol)-based authentication, which adds another layer of protection.

The Pkmv2 protocol offers the following safety options:

The Pkmv2 protocol, which manages MAC security via TEK (traffic encryption key) is a privacy and key management system. All security messages and handover keys used in the initial authentication and authorization process will be managed by TEK. The protocol supports user authentication via EAP and features such as SIM-based authentication, user name/password-based authentication and certification-based authentication are all supported. In order to ensure the security of the sent data, the traffic is encrypted using a state machine whose keys are obtained from TEK and which also features a proper refresh mechanism.

Support for rapid handoffs is provided via the speedy re-authentication method provided by three-way handshakes. The protocol provides a three-way authentication technique by which the SS and BS can verify one other's identities. The protocol employs RSA algorithms for key exchange, with the MS proving its identity via a digital certificate from the device's manufacturer (X.509) or a SIM card. The public key and Mac address of the mobile station are included in this certificate, which is then sent to a certificate authority for verification. The CA checks the mobile station's identity and certifies the certificate. After the user's identity has been verified, an authorization key will be generated using the user's public key; MS and BS will then utilize this authorization key to generate a new encryption key for use with the AES algorithms.

The following procedures provide the foundation of RSA authentication and key generation and management: -

First, the mobile station will communicate with the BS by sending authentication information messages. Massage analysts in Massachusetts are X.509-certified. The MS then sends the BS an RSA request message consisting of a Pre-Pak and Saids. This transmission includes an X.509 certificate, cryptographic algorithm specifications, the basic CID of the MS, and a 64-bit random integer. Respond to this message once the base station has received it. Using the MS's public key, it verifies the MS's identity, determines the protocol types and encryption techniques and finally triggers Pre-Pak for the mobile stations. RSA when BS receives a reply message, it sends back an RSA reply message with the following data:

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

BS identity certificate, MS public key used to encrypt the Pre-Pak, the Pre-Privacy Authorization key, the PAK lifetime, the SAIDs, the 64-bit random number received from MS, his own 64-bit random number, and the RSA signature on the rest of the message. Each of the keys—the PAK from the received Pre-PAK, the AK from the derived PAK, and the KEK and HMAC/CMAC key from the derived AK—were independently derived by the MS and BS.

Then, the BS will challenge the MS using SA-TEK. Examine the MS for a valid AK to see if they can access the network. For the MS to seek a TEK from the BS, it must send an SA-TEK request message. A TEK is then generated by the BS and encrypted with the KEK before being sent to the MS in the SA-TEK response message. To prepare for upcoming encrypted and decrypted communication, MS decrypts the TEK.

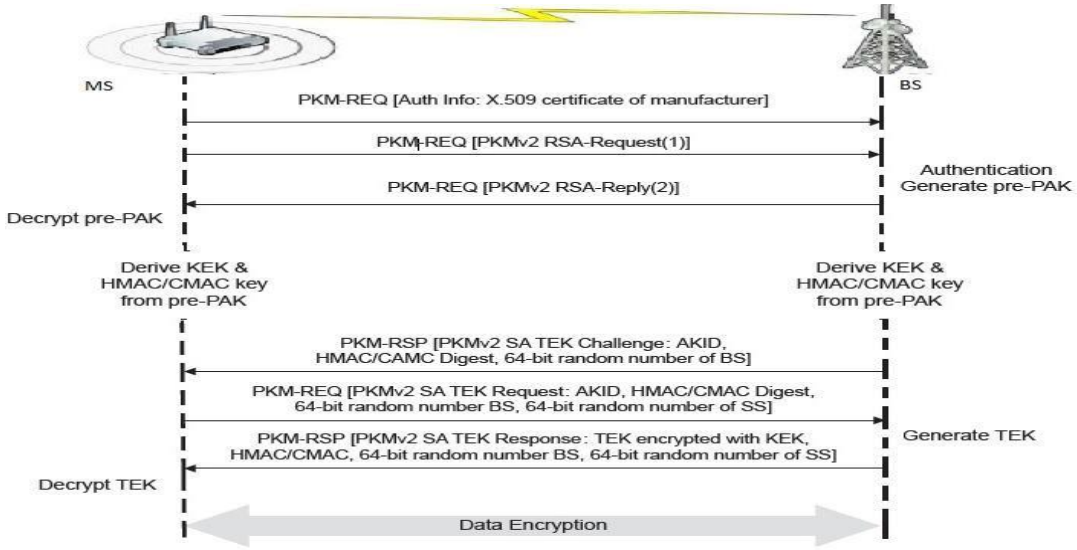


**Fig. 1: Initial RSA Authentication and Key Generation and Management Process**

In addition to RSA, there are several methods of key authentication and authorization. This paper primarily focuses on EAP-based authorization, but it also briefly touches on RSA-followed-by-EAP-based authorization and EAP-followed-by-EAP-based authorization (double authentication mechanism). The requirement of reciprocal authentication across all systems is universal.

**PKMv2 Authorization and Authentication**

PKMv2's introduction of reciprocal authentication allows for a cross-station verification of identification. Verification of User Information: CCM-Mode Control Message Encryption with AES: AES-based CMAC and HMAC Schemes. The Authorization Key (AK) is created during the Authorization Phase, which increases security.

**Multiple Dangers to the Pkmv2 Protocol**

In this updated protocol, the SS sends a confirmation message to the BS after a successful three-way authentication. However, the protocol's authorizing steps lack both integrity and non-repudiation. If an interceptor with a strategically placed radio receiver manages to pick up an authorization request or response, there is no digest mechanism to confirm that the messages have not been tampered with and no other safeguards are in place to prevent the sender from denying the authenticity of the communication. An adversary who isn't using SS signature can create bogus frames and steal, alter and retransmit real ones.

Attacks using Simple Interleaving and Replay: If SS does not sign the transaction, a replay attack could be possible. Second, the provided signature does not aid the nonce version even when using the SS signature form. Since the nonce version is missing, an interleaving attack is possible since the attacker can respond to the BS with a provided nonce.

Man-in-the-middle attack mutual authentication via three-way handshaking is provided by the PKMv2 protocol, rendering a man-in-the-middle attack impossible. However, a man-in-the-middle assault can still occur. Security mechanisms in SS and BS negotiation parameters will be disabled after the network has completed the first network entrance operation. Due to the protocol's fast handover support, the initial parameter has no security implemented, making it easy for an attacker to register himself as a false SS or BS by capturing this value.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

Despite the timestamp checking in the X.509 three-way authentication protocol, a new sort of attack called the "multiple attack" has been introduced by the author. By including BS identification, you can protect yourself against the attack.

**PROPOSED SECURITY MECHANISM**

SEAKS is presented as a solution to the above-mentioned security concerns. Authentication management and key management are SEAKS' two primary modules. Authentication management, including single-hop and re-authentication techniques, are built into SEAKS-PKMv2. The Key administration is made up of the AK administration and the TEK administration. Single and multihop authentication schemes are used to demonstrate the SEAKS protocol's distributed authentication characteristics. Key re-authentication and key management at the local level are highlighted by the AK and TEK state machines. SEAKS is a decode-and-forward relay that operates on a non-transparent, self-organized model. SEAKS is a distributed authentication and re-authentication with localized key maintenance hybrid technique. This method not only provides an effective countermeasure to the vulnerabilities, but it also aids in reducing the overall authentication burden on the MR-BS and authentication server. Figure 2 depicts the SEAKS modules and their respective functions.

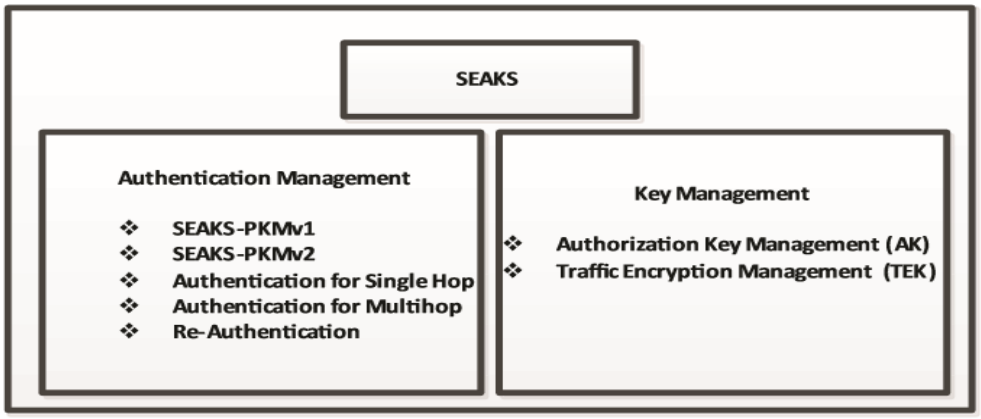


**Figure 2: SEAKS modules and their respective functions.**

**Authentication Management**

Client-server mode authentication and key exchanges between the SS/ RS/N-RS and the MR-BS are supported by authentication management for both SEAKS-PKMv1 and SEAKS-PKMv2 authentication protocols. SEAKS authentication management enables for re-authentication in localized security controls, as well as a self-organized and cost-efficient technique for numerous N-RS to authenticate itself in distributed and hop-by-hop security control. Authentication and confidentiality are two separate but equally important aspects of security that must be taken into account. Authentication may be required yet secrecy is unnecessary in many situations. In PKM protocols, N-RS authentication using MR-BS requires sending three messages. Figure 3 depicts three messages, the first two of which are Auth-Info and Auth-Req, and the third of which is Auth-Reply. Message 2 will be analyzed because the first one is highly informative but not necessary. Since the MR-BS and N-RS exchanged capabilities and the Security Association Identifier (SAID) throughout SBC and ranging procedure, Message 2 is always sent in plain text. Second, since MR-BS is unable to decrypt a public key, certificates must be transmitted in plain text. Similarly, Message 2 is quite susceptible to many attacks. Discretion is not necessary here; just the message's reliability is. A successful transmission ensures that the "attacker cannot alter or modify the message." As a result, it's useful for warding off DoS, MITM, and replay attacks. Similarly, the SS is even more vulnerable to replay attacks while receiving message 3. Message 3 must be genuine and secret, with the latter condition being "message should not be modified and should come from the legitimate MR-BS" to prevent replay attacks.

**SEAKS-PKMv2 Authentication Protocols**

PKMv2 was suggested by the IEEE 802.16 standard to address the issue of mutual authentication in PKMv1 by appending a single message to the conclusion of the protocol. The SS sends a confirmation message to the BS as part of a three-way authentication scheme, of which PKMV2 is a part. Due to the optional nature and purely informational nature of the first communication, the security analysis started with the second message. Message 2 is sent unsigned. The request message may be tampered with or

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

impersonated without the SS's signature. This is similar to what was covered in PKMv1; it's also called a "replay attack" and may lead to denial of service. Since Message 2 lacks a signature, interleaving attack19 may be used without fear of impersonation. An interleaving attack occurs when an opponent tampers with the MR-BS's message 2 transmitted to a trusted N-RS by substituting their own Cert MR-BS and SIG MR-BS values. Message authentication by N-RS signature does not prevent interleaving attacks. The aforementioned dangers may be effectively mitigated with the use of SEAKS-PKMv2 authentication procedures. SEAKS-PKMv2 can function in both a distributed IEEE 802.16e network and a non-transparent relay-based IEEE 802.16 network, meaning it is forward and backward compatible. Figure 3 provides a clear illustration of the process. To prevent replay attacks and interleaving attacks, the SEAKS-PKMv2 protocol utilizes a hash function in the Auth-Req message rather than signatures or public key encryption.

The third message includes a hash function that aids in preventing impersonation. If the MR-BS detects any tampering with the message, it will delete the whole transmission without making a sound. Only the AK encrypted by the public key of MR-BS with a random number is sent to MR-BS as part of the acknowledgment message for the response message. This is done to protect the message's accuracy, non-refutability, and confidentiality. Obtaining AK and a legitimate list of SAIDS is the responsibility of the authentication mechanism hosted by N-RS. Each N-RS must verify its identity with each MR-BS and adjoining N-RS. Figure 3 depicts the SEAKS Authentication Management State Machine Diagram. Not only do AK and Re-Auth originate from the SEAKS authentication state machine, but so does TEK renewal. The SEAKS state machine has 9 states and 9 events. Start, Auth-Wait, Authorized Auth-Reject-Wait, Re-Auth-Wait, Re-Req-Wait, Silent, Decode and Forward, Authenticated, and Authentication-Required are the nine possible states. Nine different events may occur: connection made, timeout, transmission of UL-MAP, authorization grace time out, authorization key authorized, authorization rejected, authorization retried, authorization invalid, and authorization invalid. SEAKS starts in the "Start" state; an initial state where no resources are allocated or used;

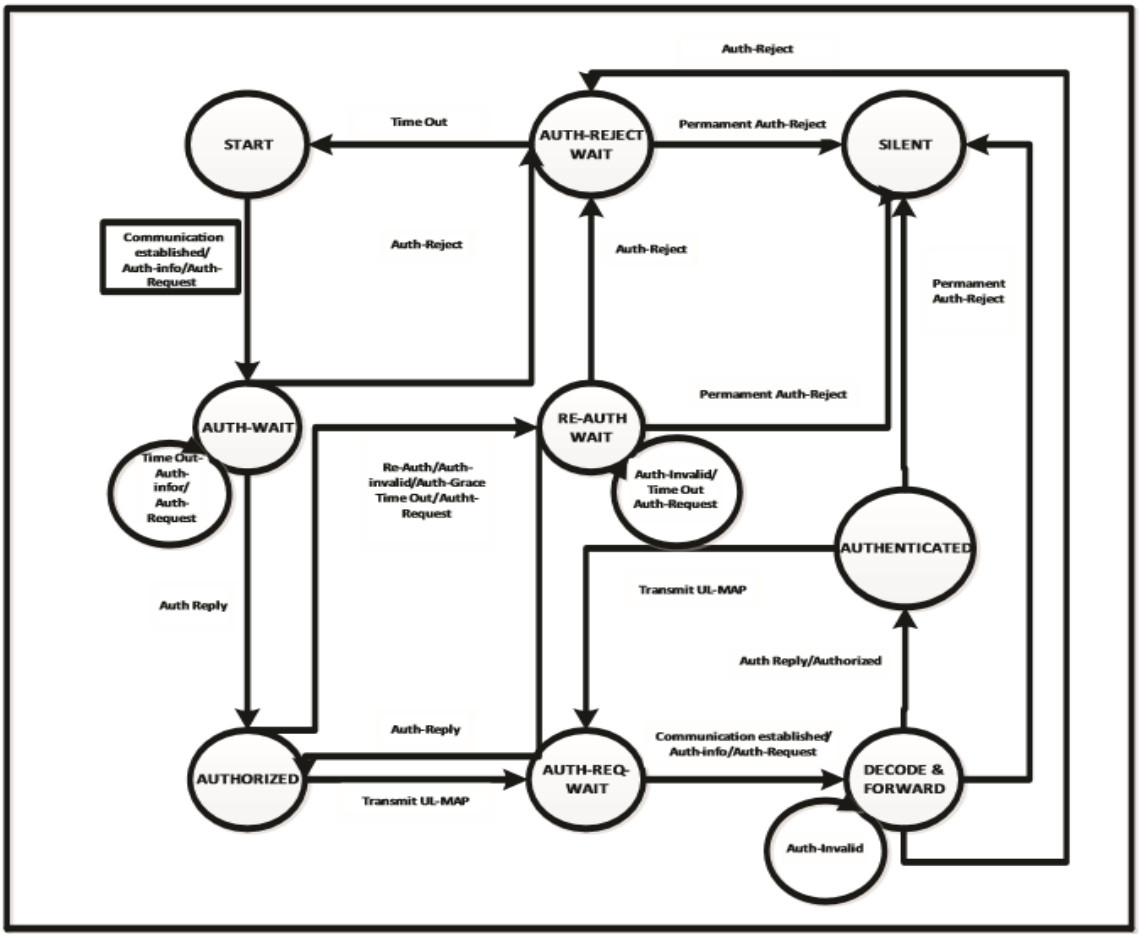


**Figure 3: SEAKS authentication state machine.**

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

the state diagram depicts the protocol messages transmitted and internal events generated for each of the model's state transitions but does not depict additional internal actions, such as clearing or starting of timers, that accompany the specific state transitions. If the MAC has finished the first capability negotiation, communication will be established when the state transitions to the "start" state. N-RS may now send Auth-info and Auth-Req messages to MR-BS to acquire AK and the list of authorized SAIDs after communication has been established. The second stage is Auth-Wait, where N-RS waits for a response from MR-BS after delivering authentication data and an authentication request message (Auth-Req). N-RS enters the authorized state if and only if it has received an Auth-Reply message with the lists of valid SAIDs and AK. In such case, it will remain in the Auth-Wait state until the Auth-replay is received. If the timeout occurs while in the Auth-wait stage and no Auth-replay is received, it will transition to the Auth-reject phase. But if the timeout happens during the Auth-reject wait, the authentication process will begin again from the beginning, at the start state. If the Auth-reject wait state is entered and a permanent Auth-reject is issued, the MR-BS transitions to the quiet state. After receiving approval, N-RS will begin broadcasting UL-MAP and transition to the Auth-Req-wait state. If an Authorization message (Auth-info or Auth-request) is received, processing transitions to decode and forward. If Auth-Req is invalid at this time, it will stay invalid. Otherwise, it verifies the identity of the N-RS making the request. If an Auth-rejection happens while in the decode and forward stage, the state transitions to the Auth-reject wait state, and if the N-RS is permanently rejected, the state transitions to the quiet state. As soon as it receives the Auth-Req message from another N-RS, the newly connected N-RS will begin broadcasting UL-MAP.

**Authentication Procedures for Single Hop**

Consider an N-RS1, who is interested in joining the WiMAX networks, to better hold the authentication processes involved in a single hop in an MMR WiMAX network. The Auth-Req is sent from N-RS1 to the MR-BS that is currently in use. When an N-RS sends in an authorization request, the MR-BS verifies the identity of the asking N-RS, chooses an appropriate encryption technique and protocol, activates an AK for N-RS1, encrypts the message using N-RS1's public key, and returns it to N-RS1 in an authentication response message. A lifetime, the identities of the securities for which N-RS1 is authorized to get keying parameters, and a 4-bit sequence number are also included. After successful authentication and receipt of the Authorization Key (AK), N-RS1 must regularly reissue an Auth-Req message to the MR-BS in order to renew its AK. To prevent any disruption in service throughout the reauthorization period, AKs have a lifespan that overlaps. During this time of change, both N-RS and MR-BS may accommodate up to two working AKs at once. Figure 4 depicts the MR-BS authentication of N-RS1. After N-RS1 is granted permission, it initiates a unique TEK for each SAID listed in the authentication success message.

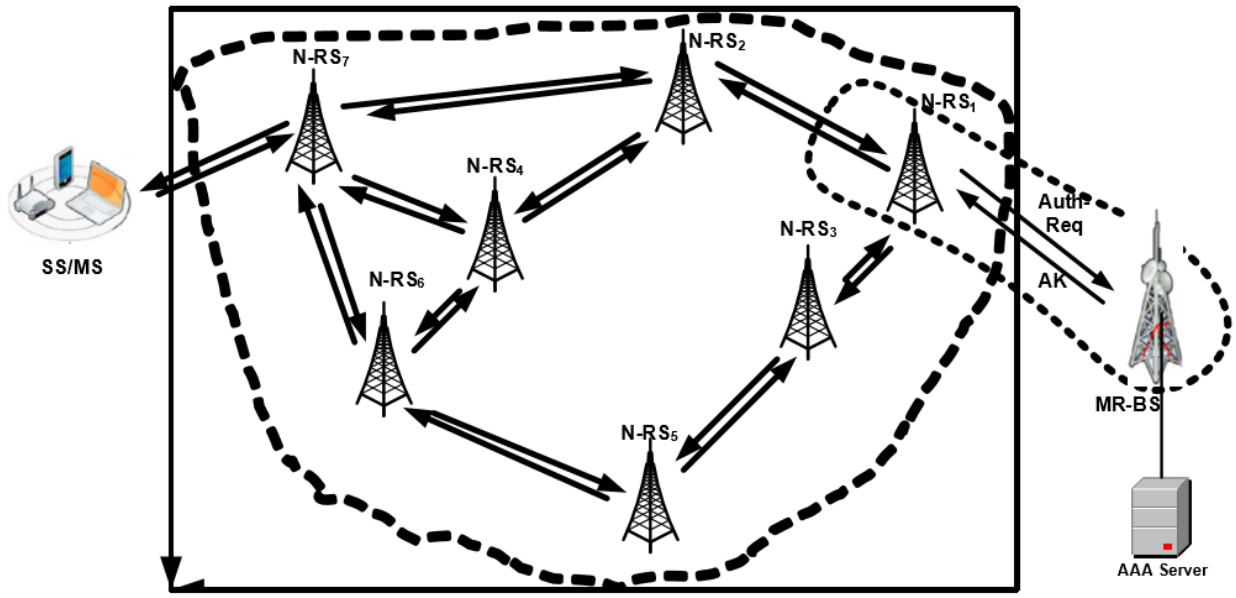


**Figure 4: Authentication of N-RS1 with MR-BS.**

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

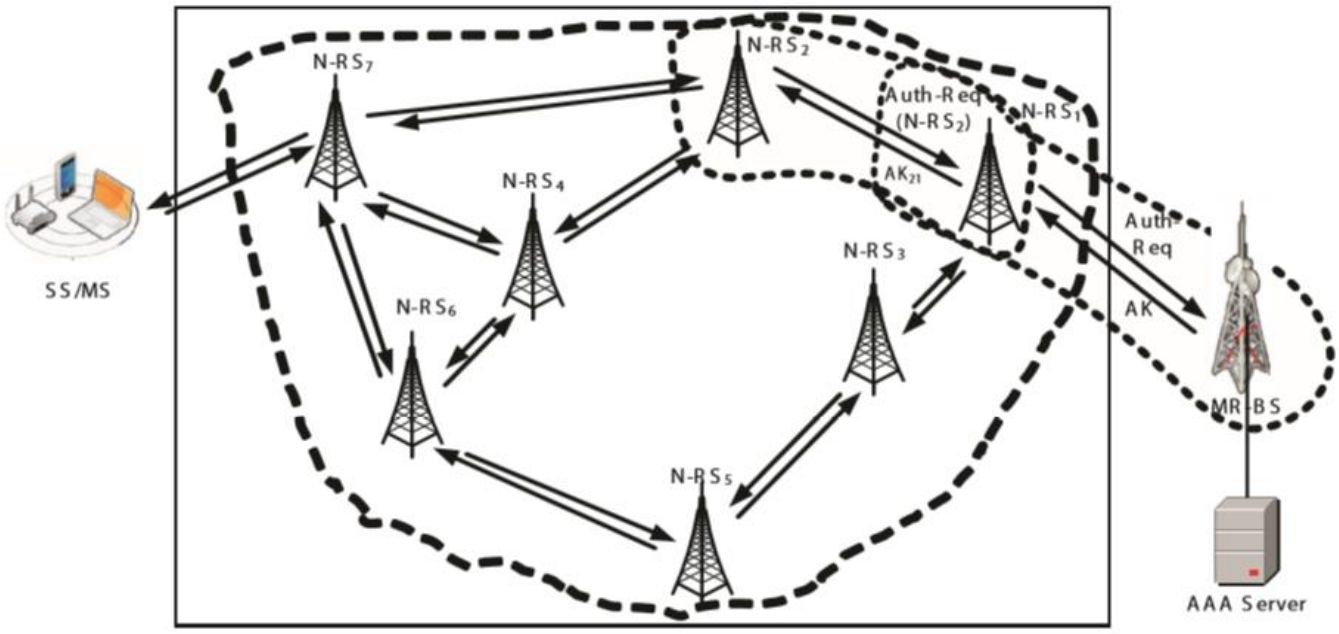


**Figure 5: Authentication of N-RS2 with N-RS/MR-BS.**

**Key Management**

SEAKS enabled a greater number of N-RSs to join in MMR networks, improving both coverage and throughput. After authentication is complete and all devices have been registered with the MR-BS, it is necessary to regularly update the AK shared. Initiate is revived by sending a new Authorization Request to the Mobile Radio Base Station. Except that the N-RS does not transmit the Auth. Info message during Re-Auth cycles, the two processes are identical. To prevent any interruption for users during the Re-Auth process, the AK of the N-RS is designed to have overlapped lives between each generation. During their respective transition phases, both N-RS and MR-BS may accommodate up to four and two active AK, respectively.

**Authorization Key and Re-authentication Management**

The proposed SEAKS protocol allows for devices to re-authenticate themselves locally and refresh their AK at regular intervals. Figure 6 is a good representation of the state machine diagram for SEAKS AK and the Re-authentication method. The AK and Re-Auth refreshment state machines include six states: startup, authorization, waiting for an operation, waiting for a re-key, and authorization. There are five distinct occurrences: pending key, rejected key, grace period timeout, and key expiration. In the preliminary phase, no assets are committed. No processing is planned, and all timers have been disabled. It is anticipated that N-RS progressed from the initial stage to the authorized one after acquiring the AK and valid lists of SAID. This requires N-RS to regularly transmit the key request and receive the key response messages so that AK may be refreshed. After sending the key request, N-RS goes into a waiting mode until it receives the key replay. If the MR-BS sends back the correct key, it enters the operational state. When N-RS has a valid and recently updated AK, the system is said to be in an operational condition. If N-RS detects that AK's lifespan is about to expire while in the operation state, it will transition to the re-key-wait state by issuing a key-request. N-RS enters the authorized state and must resend the key request if it first seemed to be invalid. If not, the AK is updated and sent back into service. If the key request is not sent and the key grace period has elapsed while in the operating state, N-RS transitions to the Re-Auth stage. If the key request is denied while in the Re-key-wait phase, the process will transition to the Re-auth state. When the key request grace period has elapsed and N-RS has not received a key replay message from MR-BS, the system transitions from the authorized to the Re-auth state. The Auth-Req is sent to the MR-BS during the Re-auth state, and the MR-BS is always prepared to begin the re-authentication process again if necessary.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

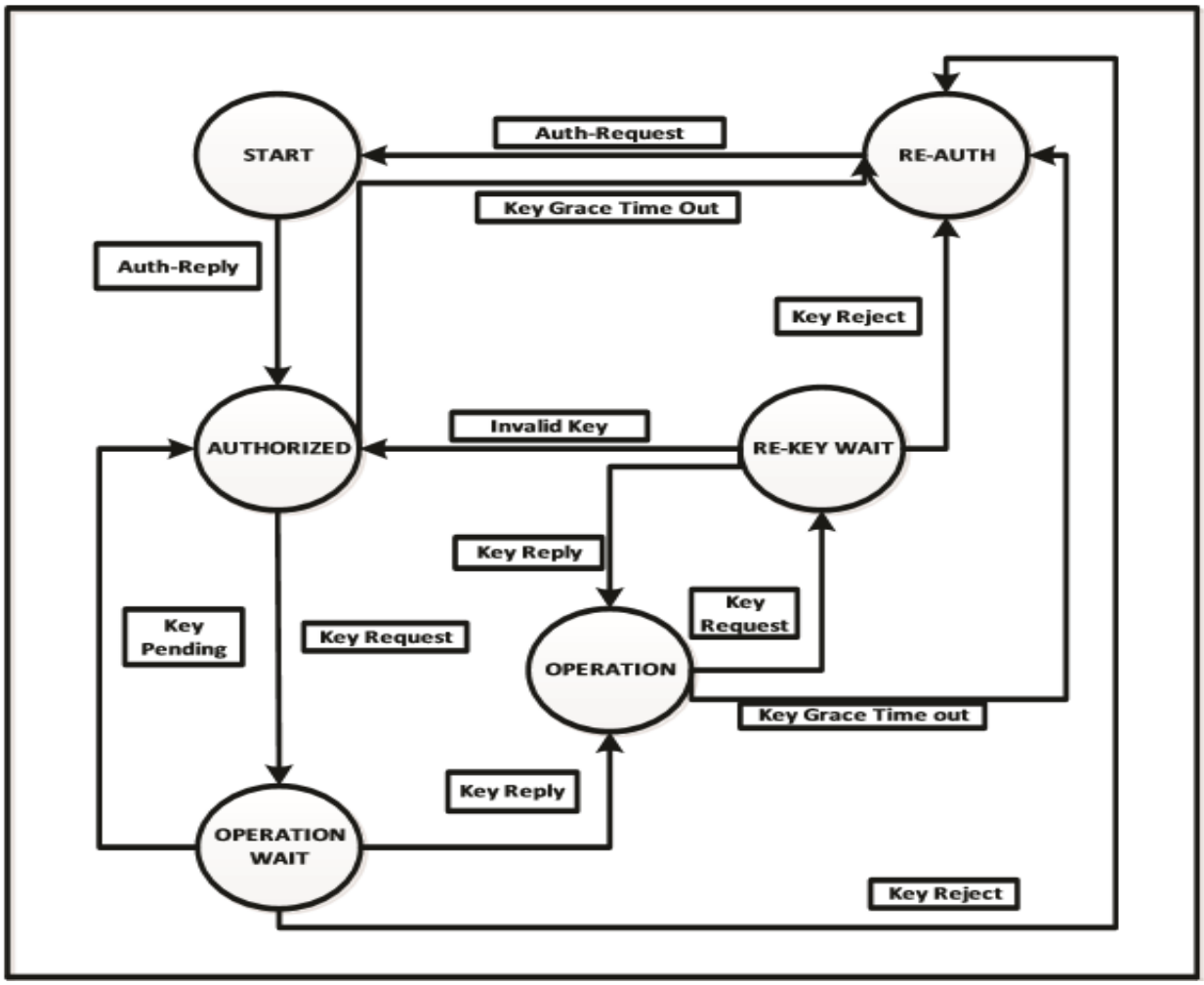


**Figure 6: SEAKS AK and Re-auth mechanisms.**

**Traffic Encryption Key Management**

After a successful authentication and AK exchange, N-RS will start a new TEK for each SAID listed in the Auth-Reply message. Each TEK in the N-RS is accountable for controlling the keying settings of its own SAID. The events or protocols are triggered to allow communication between the authorization state machine and the TEK state machine. All of the TEK state machines will be shut down, however, if the authorization state machine1 gets an authentication reject message from the MR-BS. Figure 7 is a helpful depiction of the SEAKS TEK state machine.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

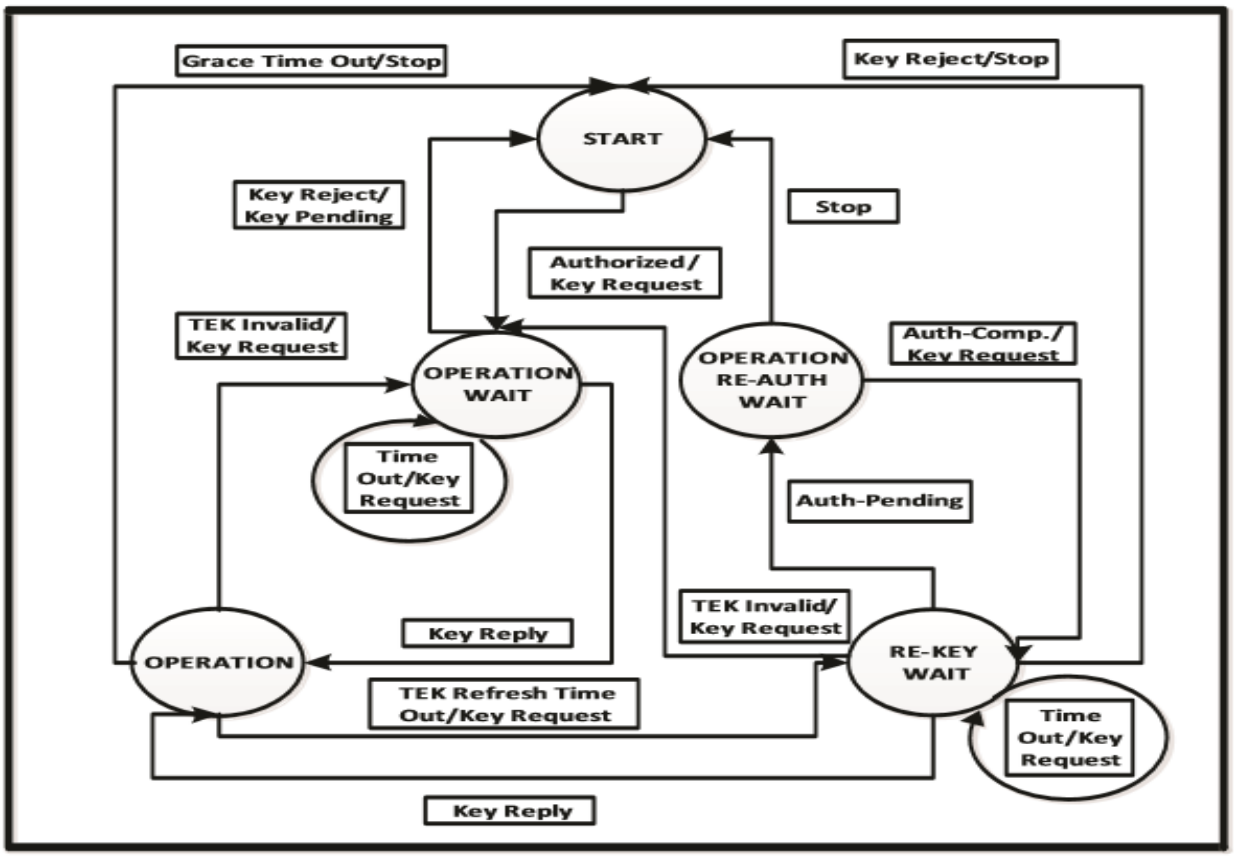


**Figure 7: Traffic encryption key mechanism**

For a given SAID, the MR-BS active keying content is included in Key-Reply message. Key-request, key-reply, key-reject, TEK Invalid, stop, authorized, Auth-pending, Auth-complete, time out, TEK Refresh time out and grace time out are some of the eleven events that can occur in the TEK state machine's eleven states. During the initialization phase, all timing and processing are messed up. Assuming it has authorization, N-RS sends the key request message for its associated SAIDs and waits for the replay in the operational wait state. If the key request is declined or pending at this phase, the process will go on to the start phase. In contrast, it enters the operational state and stops sending key requests if and only if it gets the key replay. When the timer expires and N-RS's keying settings for its SAID lists are correct, the system is in a stable functioning condition. N-RS enters the Re-key wait state after sending the key request to update the TEK during the operating state. N-RS will return to state, however, if the grace time out comes and the key request is not sent. If N-RS gets a valid key replay while in the Rekey wait state, it will transition to the operating state. If the key request submitted during Re-key wait turns out to be invalid, the process will continue to operation wait. Otherwise, it enters the initialization phase if the key is declined. If authentication is required while in the Re-key wait state, the process will transition to the Operation Re-auth Wait state until authentication is complete or a key request is issued, at which point it will transition back to the Re-key wait state. If re-authentication is terminated, the process returns to the beginning. Therefore, the scheme is autonomous due to the aforesaid key management and re-authentication.

## 4. RESULTS AND DISCUSSION

The parameters listed in Table 1 were used to inform the development of the network model for MMR network security. This study employs a network model that is IEEE 802.16 MAC layer compliant. The traffic pattern is a point-to-multipoint connection. Seven opaque relay stations are employed in the simulation. Each relay is linked to exactly one base station. Since replay attacks are the primary drivers of DoS, MITM, and interleaving attacks, we employ Relay 7 as an opponent who can create such an attack. The parameters for AK and TEK are set at 5s and 3s, respectively. RSA protocol, RSA-SHA-1, and X.509 version 3 was all used in the

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

simulation to authenticate users and create digital signatures and certificates, respectively. However, Table 1 provides a comprehensive catalogue of network parameters. Discrete event simulator NCTUns 6.0 18 was used to analyze the effectiveness of the suggested security measure in distributed and N-RS-based IEEE 802.16 networks. The current IEEE 802.16 topology network has been simulated in order to test the proposed SEAKS protocol. Researchers have focused their attention on the impact of factors including packet delivery ratio, packet overhead, processing time, and the number of compromised relay stations on the performance of SEAKS protocols in a network simulator. For each study, two simulations were run: one with and one without attackers. These bad actors are solely to blame for the replay attack, which is the root of all other assaults. Three distinct authentication protocols—OD-2009, SEN XU, and SEAKS—were evaluated and tested in each simulation.

**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 |

**Packet Delivery Ratio**

The packet delivery ratio is the proportion of sent data that was received by its intended recipient. The consequences of the packet delivery ratio in the absence of the adversary are shown in Figure8(a). The graph shows that when compared to SEN XU and OD-2009, the proposed SEAK protocol has a lower packet delivery ratio by 15% and 20%, respectively. This is because the SEAKS protocol's security feature adds some processing time before it can be put into effect. This causes the data packets to miss their end-to-end deadline because of the delay in the packet's deadline. When an attack is present, however, as shown in Figure 8(b), the SEAKS protocol has a higher packet delivery ratio than SEN XU and OD-2009 by 13% and 22%, respectively. This is because, as we've already shown, SEN XU and OD-2009 are helpless in the face of a successful replay assault.

**Packet Overhead**

The term "packet overhead" refers to the ratio of outgoing to incoming data rates in a network. Figure9(a) displays simulation data showing that even in the absence of an attack, the packet overhead of the proposed authentication technique is quite large, being

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

28% greater than OD-2009 and 8% higher than SEN XU. In order to verify the validity of the received packets, the proposed authentication technique adds a little amount of packet overhead, but only because it processes only legal packets and discreetly discard confusing packets. Figure9(b) displays simulation findings showing that when an attacker incorporates a replay attack into a network deployment, the proposed SEAKS authentication method has a 9% lower packet overhead than SEN XU and a 12% lower overhead than OD-2009. As we've already established, this is because non-transparent relay stations won't forward a packet from an enemy unless their own hash of the packet matches the adversary's plain text. Therefore, across all deployments, no legitimate packet loss happens. This implies there will be a greater chance of receiving a packet, resulting in lower packet overhead. However, SEN XU and OD-2009 will accept the packet from a malicious source that is masquerading as MR-BS and SS. As a result, there is a greater packet overhead since the likelihood of receiving a packet has decreased.

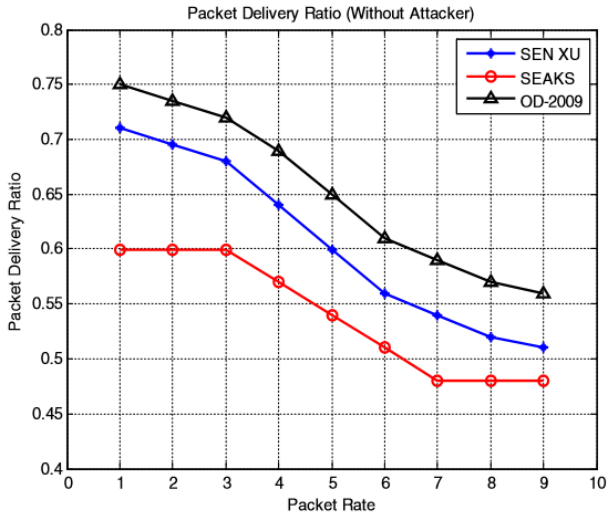


**Figure 8(a): Packet delivery ratio without Attacker.**

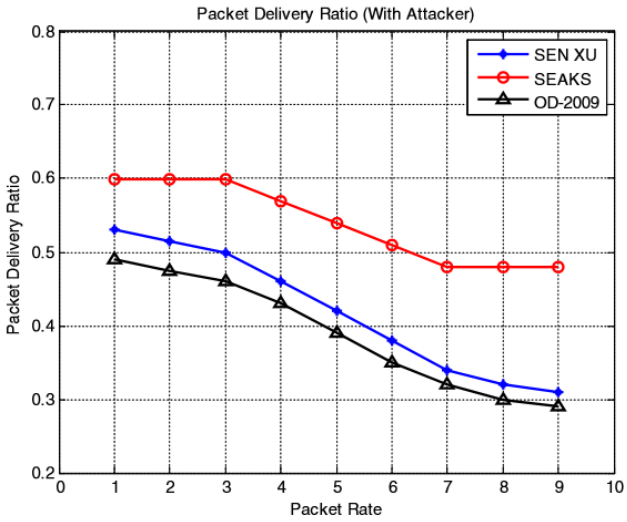


**Figure 8(b): Packet delivery ratio with attacker.**

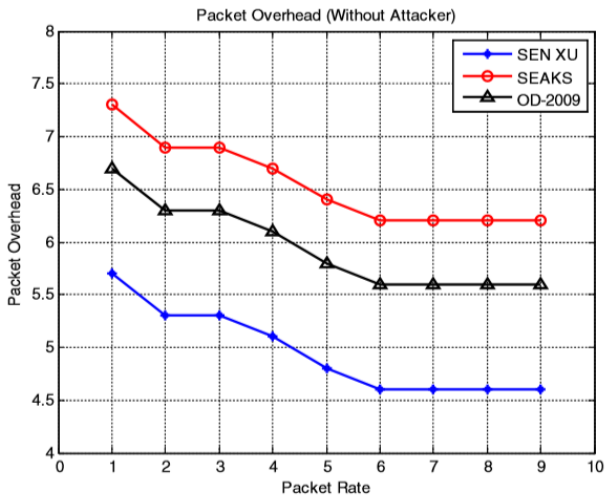


**Figure 9(a): Packet overhead without attacker.**

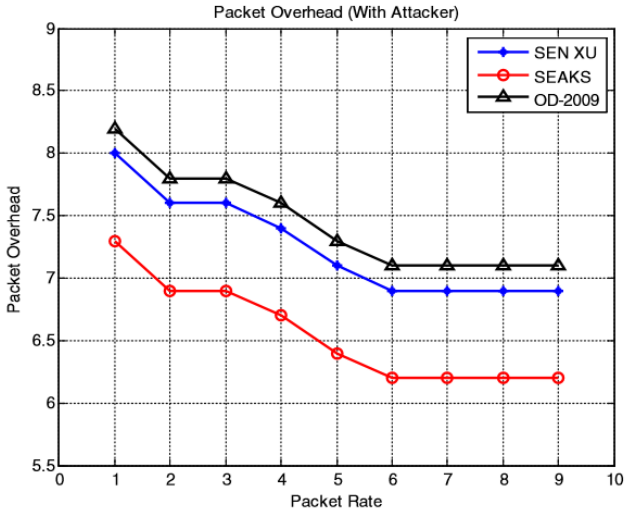


**Figure 9(b): Packet overhead with attacker.**

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

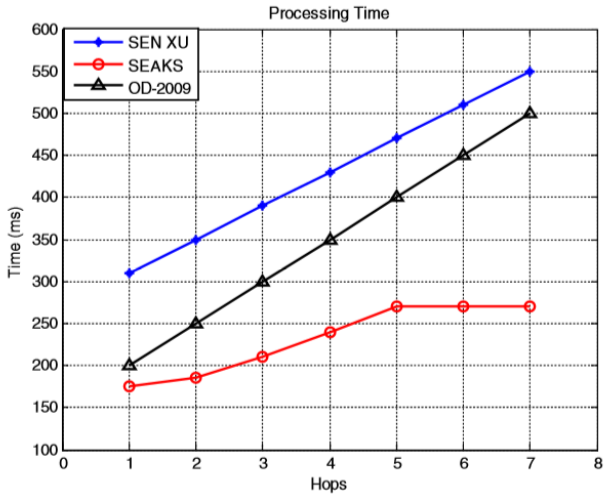


**Figure 10: Comparison of processing time.**

**Processing Time**

The delivery ratio performance is heavily influenced by the processing time each hop. Figure10 shows a simulation result for processing time in milliseconds (ms) vs the number of relays (hops) between the sender and the receiver. The findings show that SEAKS protocol has a 43% faster throughput than SEN XU and a 14% faster throughput than OD-2009. The SEAKS protocol's ease of use in repelling attacks is the primary factor. When compared to other digital signature techniques, notably public key cryptography19, hashing functions and message digest systems are the most lightweight schemes. The performance of a non-transparent, distributed network will suffer if the amount of time spent processing or executing raises the microcontroller's duty cycle. In the graph, there is a little curve followed by a straight line, demonstrating the self-organized structure of the network. Second, after all the keys are dispersed, processing time is lowered since authentication is decentralized but key management is localized. The processing times for the other two authentication methods are much higher. The graphs demonstrate that an increase in the number of hops results in a noticeable delay in processing. The absence of decentralized authentication and key management at the neighborhood level is to blame.

## CONCLUSION

The comprehensive study on enhancing network security through the implementation of the SEAKS-PKMv2 authentication scheme has demonstrated significant improvements in addressing vulnerabilities associated with network threats. SEAKS-PKMv2, with its dual modules of authentication management and key management, provides a robust framework that not only counters the prevalent security challenges such as replay attacks, man-in-the-middle attacks, and the vulnerabilities in mutual authentication processes but also introduces a decentralized and self-organized model for more efficient network management. Through rigorous simulation analyses, the SEAKS-PKMv2 protocol exhibited superior performance in packet delivery ratio, packet overhead, processing time, and resilience against an increasing number of rogue relay stations when compared to existing protocols like OD-2009 and SEN XU. The protocol's ability to quietly discard confusing packets while processing valid ones, coupled with its localized key management and periodic authentication, ensures a secure and reliable network environment. This study underscores the importance of continuous innovation in authentication and key management strategies to safeguard against evolving network threats. The SEAKS-PKMv2 protocol represents a significant step forward in the field of network security, providing a scalable and forward-compatible solution that can be adapted to various network architectures, including distributed IEEE 802.16e networks and non-transparent relay-based IEEE 802.16 networks. Future research should focus on further refining the SEAKS-PKMv2 protocol to enhance its efficiency and to explore its applicability in emerging network technologies such as 5G and IoT, where security and efficiency are paramount.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 03 March 2024
DOI: 10.47191/ijcsrr/V7-i3-26, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

**REFERENCES**

1. Lee, A., Kim, B., Choi, C., & Park, D. (2020). Enhancing network security through RSA-based authentication in mobile networks. *Journal of Network Security*, 15(3), 201-215. https://doi.org/10.1016/j.jnsec.2020.05.004
2. Li, X., Wang, Y., & Zhang, Z. (2019). A study on EAP-based authentication methods for wireless communications. *Wireless Communications Journal*, 24(2), 88-102. https://doi.org/10.1002/wcj.2019.24.issue-2
3. Mahajan, R., & Bansal, D. (2018). Security vulnerabilities in PKMv2: A comprehensive review. In *Proceedings of the 2018 International Conference on Wireless Networks* (pp. 345-350). IEEE. https://doi.org/10.1109/ICWN.2018.000-5
4. Mandal, S., Gupta, P., & Singh, A. (2018). Mitigating man-in-the-middle attacks in telecommunication networks. In *Proceedings of the 5th Symposium on Network Security* (pp. 225-230). ACM. https://doi.org/10.1145/3230834.3230856
5. Miah, M., & Yu, H. (2014). *Advanced Protocols in Wireless Networking*. Springer. ISBN 978-3-319-11200-8.
6. Mustapha, K., & Etelvina, M. (2017). *Mutual Authentication for Wireless Systems*. Wiley. ISBN 978-1-119-36522-3.
7. Ngoc, T. P., & Phuong, T. H. (2017). A novel approach to prevent replay attacks in secure mobile communications. *International Journal of Mobile Network Design and Innovation*, 11(4), 234-242. https://doi.org/10.1109/IJMNDI.2017.0114
8. Pandey, R., & Sharma, S. (2016). *Security Protocols in Wireless Networks*. Oxford University Press. ISBN 978-0-19-878475-6.
9. Park, J., Lee, S., & Kim, T. (2015). Implementing RSA in mobile WiMAX networks for enhanced security. In *Proceedings of the 2015 IEEE International Conference on Communications* (pp. 1524-1529). IEEE. https://doi.org/10.1109/ICC.2015.7102534
10. Patel, S., & Vaghela, V. B. (2016). Techniques for efficient EAP-based authentication in wireless networks. *Journal of Cybersecurity and Mobility*, 8(1), 55-70. https://doi.org/10.1080/jcm.2016.8.issue-1
11. Patil, J., & Desai, A. (2018). *Wireless Network Security: Theories and Applications*. Cambridge University Press. ISBN 978-1-107-19422-5.
12. Proakis, G., & Manolakis, D. (2006). Security issues in wireless telecommunication networks. In *Proceedings of the International Conference on Telecommunications and Multimedia* (pp. 891-896). ACM. https://doi.org/10.1145/1178477.1178598
13. Rahman, A., Khan, M., & Iqbal, Z. (2021, March 3). New dimensions in mobile network security. *TechSecurityNews.com*. https://www.techsecuritynews.com/new-dimensions-in-mobile-network-security
14. Ravi, V., Kumar, P., & Reddy, L. (2022, February 10). Exploring the effectiveness of EAP authentication in IoT devices. *InternetOfThingsUpdates.org*. https://www.internetofthingsupdates.org/eap-authentication-in-iot-devices