Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Enhancing Security Authentication in Mobile Ad Hoc Networks (MANETs) Using ETESLA-ACK

[1] D. Vijaya Kumar, [2] Dr. C. Chandrasekar

[1] Research Scholar, Department of Computer Science, Government Arts College Udumalpet - 642 126, India.
[2] Head, Department of Computer Science, Government Arts and Science College, Mettupalayam - 641104, India.

Abstract - Security authentication in Mobile Ad Hoc Networks (MANETs) remains a critical challenge due to their decentralized and dynamic nature. This research proposes an enhanced authentication scheme leveraging ETESLA-ACK (Enhanced Timed Efficient Stream Loss-tolerant Authentication with Acknowledgments). Nodes in the MANETs generate Authentication Tokens (AT) containing message payloads, expiration times, and digital signatures. Recipient nodes verify tokens to ensure message relevance and authenticity. Periodic key renewals and group key updates bolster security. This approach enhances MANET security by providing robust authentication, message integrity, and secure key management while mitigating vulnerabilities. Simulation results demonstrate its effectiveness in safeguarding MANET communications.

Keywords: MANETs, Security Authentication, ETESLA-ACK, Authentication Tokens, Key Management, Message Integrity, Mobile Ad Hoc Networks.

1. Introduction

Mobile advertising has permeated every aspect of research everyday lives in the current digital era. Whether you're scrolling through social media, playing mobile games, or browsing your favorite apps, chances are you've encountered mobile advertisements. These ads are not only a source of revenue for app developers and businesses but also a way for consumers to discover new products and services. However, with the increasing prevalence of mobile advertising, there comes a growing concern for security and privacy. How can it ensure that the ads sees are from legitimate sources and that research personal data remains protected? This is where the concept of security authentication in the context of mobile advertising and High Order Bits (HOB) networks becomes crucial.

In the ever-evolving landscape of mobile advertising, the concept of security authentication within the context of a highly dynamic ad hoc network plays a pivotal role in safeguarding both user privacy and the integrity of the digital ecosystem. With the proliferation of smart phones and mobile applications, the seamless integration of advertisements into research daily digital experiences has become increasingly prevalent. However, this convenience comes with a pressing need to ensure that the advertisements users encounter are not only relevant but also trustworthy. Security authentication in mobile ad hoc networks serves as the guardian of this trust, employing sophisticated protocols and mechanisms to verify the authenticity of advertisers and ensure that users' sensitive data remains confidential. In the subsequent exploration, it will delve deeper into the intricacies of security authentication within the mobile advertising sphere, shedding light on its critical importance, the challenges it addresses, and the innovative solutions that continue to shape this evolving landscape.

2. Literature Survey

2.1 Elliptic curve cryptosystem and hill cipher (ECCHC)

Almaiah MA (2020) et.al proposed a new hybrid text encryption approach over mobile ad hoc network. The rapid increase in data exchange over mobile networks has raised significant concerns regarding the security of shared information, including text, images, audio, and video. The vulnerability to attacks and data theft on unsecured mobile channels necessitates robust encryption techniques for protection. The Hill cipher algorithm,

while known for its simplicity and fast computations, has been criticized for its weak security due to the requirement for both sender and recipient to have identical private keys. This novel approach introduces a significant advancement by allowing direct encryption of every character within the 128 ASCII table, eliminating the need for mapping tables that other methods rely on. The proposed ECCHC hybrid encryption approach combines elliptic curve cryptography with Hill cipher, transforming it from a symmetric to an asymmetric technique, enhancing security, efficiency, and resilience against potential hackers. This innovation is particularly suitable for real-time multimedia, wireless applications, and resource-constrained devices, given its simplicity and computational speed, making it a valuable contribution to secure data exchange.

2.2 Fuzzy enhanced secure multicast routing (FSMR)

Brindha V (2019) et.al proposed Fuzzy enhanced secure multicast routing for improving authentication in MANET. This research addresses the crucial need to safeguard data during transmission from both active and passive attacks within a network. While certificate-based secure routing schemes have traditionally been employed for authentication using certificates, this it introduces a novel approach called Fuzzy Enhanced Secure Multicast Routing (FSMR). FSMR is designed to elevate network and data security by identifying potential misbehaving nodes through the analysis of statistical data, distinguishing between normal and abnormal behaviors. Unlike traditional certificate-based routing, this proposed system adopts a certificate-less routing approach. It achieves data authentication through key generation, signcryption, and encryption techniques, allowing packets to be securely routed and validated without relying on certificate-based routing knowledge.

2.3 Biometric-Based Authentication

Kaur N. (2018) et.al proposed A Review of Biometric based Authentication for MANET. In today's digital landscape, security and accessibility are paramount for service providers across various domains, including social media, communication networks, and wireless networks. Users worldwide crave easy access to available resources while insisting on robust safety measures. Traditional security authentication methods often fall short in certain network transactions. Enter biometrics, a game-change in network security. Biometrics, intimately linked with individual identities, holds promise as a solution to authentication challenges in Mobile Ad Hoc Networks (MANETs). Implementing biometric-based authentication in Manet’s demands careful consideration of system constraints and security requisites. MANETs present unique challenges such as decentralized coordination and resource scarcity. Regular authentication is essential for bolstering MANET security, and biometrics offers a viable pathway by virtue of its direct tie to user identity. This research explores and discusses a biometric-based authentication mechanism, providing insights into both biometrics and MANETs along with their authentication protocols.

2.4 Data Security-Based Routing in MANETs

Bondada P (2022) et.al proposed Data security-based routing in MANETs using key management mechanism. A Mobile Ad Hoc Network (MANET) is a self-contained wireless network where mobile nodes communicate dynamically without relying on any centralized infrastructure. While offering flexibility, MANETs are susceptible to severe security threats that existing methods struggle to mitigate. The present research introduces a group key management-based routing technique that is both safe and energy-efficient. In asymmetric key cryptography, it utilizes two specialized nodes: the Calculator Key (CK) and the Distribution Key (DK). These nodes handle secret key generation, verification, and distribution, alleviating additional computation burdens on other nodes. Selection of these nodes is based on energy consumption and trust values. MANETs empower mobile users to communicate seamlessly in infrastructure-limited scenarios, but challenges such as external interference and mobility often disrupt route functionality.

2.5 Enhancing Security and Trust in MANETs

Usha MS (2021) et.al proposed Implementation of trust-based novel approach for security enhancements in MANETs. A Mobile Ad Hoc Network (MANET) is a self-contained wireless network where mobile nodes communicate dynamically without relying on any centralized infrastructure. While offering flexibility, MANETs are susceptible to severe security threats that existing methods struggle to mitigate. The

present research introduces a group key management-based routing technique that is both safe and energy-efficient. In asymmetric key cryptography, it utilizes two specialized nodes: the Calculator Key (CK) and the Distribution Key (DK). It makes use of two specialized nodes, the Distribution Key (DK) and the Calculator Key (CK), in asymmetric key cryptography. These nodes handle secret key generation, verification, and distribution, alleviating additional computation burdens on other nodes. Selection of these nodes is based on energy consumption and trust values. MANETs empower mobile users to communicate seamlessly in infrastructure-limited scenarios, but challenges such as external interference and mobility often disrupt route functionality.

3. Research Methodology

3.1 Proposed Enhancing Security Authentication in Mobile Ad Hoc Networks (MANETs) using ETESLA-ACK

Mobile Ad Hoc Networks (MANETs) are wireless communication networks where devices, such as smart phones or laptops, can connect with each other directly, without the need for a centralized infrastructure. These networks are increasingly used for various applications, including mobile advertising. However, MANETs face security challenges, and ensuring robust authentication is crucial to protect against unauthorized access and malicious activities. In this proposed methodology aim to enhance security authentication in MANETs using ETESLA-ACK, a secure communication protocol, to safeguard mobile advertising applications.

1. Understanding the Security Challenges in MANETs

Mobile Ad Hoc Networks (MANETs) face security vulnerabilities due to their dynamic, decentralized nature. Threats like unauthorized access, data tampering, and denial-of-service attacks can harm network integrity and availability. This proposed methodology aims to enhance security authentication in MANETs, focusing on securing data transmission using the Enhanced TESLA (Timed Efficient Stream Loss-Tolerant Authentication) mechanism and introducing ACK-based authentication for robustness.

TESLA Implementation

Key Generation

In the proposed methodology, "Key Generation" is a fundamental step in enhancing security authentication in Mobile Ad Hoc Networks (MANETs). Here, each node participating in the network generates a private-public key pair. The private key is securely stored and kept secret, ensuring that only the legitimate owner can access it. Conversely, the public key is shared with neighboring nodes. This key sharing establishes a foundation for secure communication within the MANET. The public keys facilitate the authentication process, enabling nodes to verify the authenticity of messages and data packets received from their peers. It's important to note that the use of asymmetric cryptography ensures that even if the public key is exposed, the private key remains confidential, preventing unauthorized access and tampering with communication.

Timestamp Synchronization

The second critical aspect of the proposed methodology is "Timestamp Synchronization." In MANETs, where nodes may join and leave the network dynamically, achieving a common understanding of time is crucial for secure authentication. Nodes synchronize their internal clocks using a common time reference or a time synchronization protocol. This synchronization ensures that timestamps associated with data packets are consistent across the network. Timestamps play a vital role in TESLA (Timed Efficient Stream Loss-Tolerant Authentication) to detect and prevent replay attacks. Accurate timestamp synchronization ensures that nodes can trust the timestamps in received packets, enhancing the reliability of the authentication process. It is essential to select a suitable time synchronization method that balances accuracy and overhead in the resource-constrained MANET environment.

TESLA Packet Tagging

To ensure data origin authenticity and integrity, the "TESLA Packet Tagging" step is employed. Data packets transmitted in the MANET are tagged with a timestamp and a MAC (Message Authentication Code). The sender's private key and the synchronized timestamp are used to create these tags. The timestamp indicates when the packet was generated, while the MAC provides a cryptographic signature of the packet contents. Together, these tags enable receivers to verify that the received packet indeed originated from the claimed sender and has not been tampered with during transit. TESLA's design ensures that this verification process can be performed efficiently, making it suitable for MANETs where resource constraints are prevalent.

Receiver Verification

The final component of the proposed methodology is "Receiver Verification." Upon receiving a data packet, the recipient node engages in a verification process. This process involves comparing the timestamp and MAC attached to the received packet with own computations. By using their synchronized clock and the sender's public key, the recipient can independently verify the authenticity of the packet. If the verification succeeds, it confirms that the packet originated from a legitimate sender and has not been altered during transmission. Receiver verification acts as the last line of defense against malicious or compromised nodes attempting to inject fraudulent data into the MANET. It ensures that only authenticated and unaltered data is accepted into the network, enhancing overall security.

Secure Data Transmission ACK Authentication

Message Digest Generation: In this phase of the proposed methodology, before transmitting data packets in a Mobile Ad Hoc Network (MANET), each node generates a message digest using a cryptographic hash function applied to the contents of the packet. The purpose of this step is to create a condensed representation of the packet's data that can be securely and efficiently transmitted to the recipient. Hash functions like SHA-256 or SHA-3 are commonly employed for this purpose. By hashing the packet contents, the sender creates a fixed-length string of characters, which serves as a unique fingerprint of the packet's data. Any minor change in the packet contents will result in a significantly different hash value, making it possible to detect even the slightest alterations or tampering during transmission.

ACK Authentication: Upon receiving a data packet in the MANET, the recipient initiates the ACK (Acknowledgment) authentication process. At this stage, the recipient generates an ACK packet containing two critical components. First, it includes the previously generated message digest, which is essentially a cryptographic summary of the received data packet. Second, the recipient signs the ACK packet using its private key. This signing process adds a digital signature to the ACK, ensuring the authenticity and integrity of the ACK packet itself. By including the message digest and signing the ACK, the recipient provides a robust mechanism to verify the received data's integrity and origin.

Recipient Verification: In the final step of this process, the sender verifies the authenticity and integrity of the received ACK packet. This verification is essential to ensure that the data transmission has been successfully authenticated. To accomplish this, the sender utilizes the recipient's public key, which is known to all nodes in the MANET. By using the recipient's public key, the sender can decrypt and verify the digital signature present in the ACK packet. If the signature is valid, it confirms that the ACK packet was indeed generated by the intended recipient and that the message digest contained within matches the digest of the originally transmitted data packet. This confirmation provides strong evidence that the data packet has reached its destination securely and has not been tampered with during transit.

Mitigating Replay Attacks

In the context of enhancing security in Mobile Ad Hoc Networks (MANETs), mitigating replay attacks is crucial. In this proposed methodology, nodes employ a proactive defense strategy to detect and discard replayed packets. This involves nodes maintaining a record of received packets and acknowledgment (ACK) messages. When a packet is received, the recipient node checks its record to ensure that it has not received an identical packet before. If a duplicate packet or ACK is detected, it is considered a potential replay attack and is discarded. This approach prevents adversaries from injecting previously intercepted and valid packets into the network to disrupt communication or deceive nodes.

Security Analysis

Security analysis is paramount to determine the robustness of the proposed security methodology against common MANET threats. This includes:

Eavesdropping: Evaluate the methodology's ability to prevent eavesdroppers from intercepting and understanding transmitted data packets. Ensure that encryption and authentication mechanisms effectively thwart eavesdropping attempts.

Impersonation: Assess the methodology's resistance to node impersonation attacks, where adversaries attempt to masquerade as legitimate nodes. Verify that TESLA and ACK-based authentication can reliably identify and reject impersonating nodes.

Data Tampering: Analyze the methodology's capability to detect and prevent unauthorized data tampering during transmission. Ensure that modifications to data packets are quickly identified and rejected.

Attack Resilience: Examine how the proposed security measures perform under adversarial conditions. Test the system's resilience against various types of attacks, including replay attacks, denial-of-service (DoS) attempts, and node compromise scenarios.

1. TESLA Authentication

TESLA is a protocol that provides loss-tolerant authentication for data streams. It is typically used to authenticate data packets in a secure manner. The key concept in TESLA is the use of one-way hash functions and timestamps to create and verify authenticators.

Create Authenticator (sender's side)

$$Authenticator = HMAC(Key, Message \,||\, Timestamp)$$

Verify Authenticator (receiver's side)

$$Computed\ Authenticator = HMAC\ (Key, Message \,||\, Timestamp)$$

If

$$(Received\ Authenticator == Computed\ Authenticator)$$

Packet is authenticated

Else

Packet is not authenticated

TESLA relies on time-based authentication. Nodes should have synchronized clocks, and packets include timestamps for verification.

Verify Timestamp (TESLA)

If $(Current_{Time} - Packet_{Timestamp} < TESLA_{Window\,Size})$

Packet is considered authentic

Else

Packet is not considered authentic

Enhancing security and authentication in Mobile Ad Hoc Networks (MANETs) using ETESLA-ACK (Enhanced Timed Efficient Stream Loss-tolerant Authentication with Acknowledgments) involves a cryptographic protocol that allows nodes to authenticate each other in a decentralized manner. Here's a step-by-step proposed algorithm for this purpose:

Step 1: Setup

1.1. **Initialization**: Each node in the MANET generates a long-term asymmetric key pair, consisting of a public key (PK) and a private key (SK).

1.2. **Shared Parameters**: Nodes share common parameters like network time synchronization and a group key (GK) known to all participants.

Step 2: Creating Tokens for Authentication

2.1. **Token Issuer (Sender)**: When a node wants to send a message, it generates an Authentication Token (AT) containing:

- Message Payload (P)
- Expiration Time (ET) = Current Time + a fixed time interval

- Node's Digital Signature (DS) on (P + ET) using its private key (SK)

Step 3: Message Transmission

3.1. **Message and Token Transmission**: The sender transmits the message (P) along with the Authentication Token (AT) to the recipient node(s).

Step 4: Receiving and Verifying Authentication Tokens

4.1. **Recipient Node (Receiver)**: Upon receiving a message and its associated Authentication Token, the recipient node performs the following checks:

4.2. **Message Relevance Check**: The recipient checks if the message is within the expiration time (ET) specified in the token. If ET has not passed, continue; otherwise, discard the message.

4.3. **Digital Signature Verification**: The recipient verifies the sender's digital signature (DS) on (P + ET) using the sender's public key (PK). If the verification succeeds, continue; otherwise, discard the message.

Step 5: Acknowledgment and Authentication

5.1. **Acknowledge Receipt**: If the message passes all checks, the recipient node acknowledges receipt of the message and its authentication.

5.2. **Re-authentication Request (Optional)**: For enhanced security, nodes can periodically request re-authentication from their neighboring nodes to ensure the continued trustworthiness of their long-term keys.

Step 6: Key Management

6.1. **Key Renewal**: Nodes periodically renew their long-term asymmetric keys to prevent compromise.

6.2. **Group Key Updates**: If necessary, the group key (GK) can be updated to maintain network security.

Step 7: Handling Compromised Nodes (Optional)

7.1. **Compromised Node Detection**: If a node suspects a neighboring node's private key has been compromised, it can request re-authentication or escalate the issue to higher authorities.

This proposed algorithm leverages ETESLA-ACK to provide secure and efficient authentication in MANETs. It ensures that messages are authenticated, relevant, and have not been tampered with during transmission. Additionally, periodic key updates and optional re-authentication requests help maintain the network's security over time.

Enhanced TESLA (ETESLA) was developed as an extension of the basic TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol to address certain limitations concerning issues with the security of data transmission in mobile ad hoc networks (MANETs). Enhanced TESLA (ETESLA) supports multiple security levels in Mobile Ad-Hoc Networks (MANETs):

Security Parameter Configuration: ETESLA allows nodes to define specific security parameters for different security levels within the network. These parameters, denoted as $HSL_{Parameters}$ for high security and $LSL_{Parameters}$ for low security, include settings such as key lengths, refresh rates, and other cryptographic parameters.

Key Length Selection: Depending on the desired security level, nodes can choose different key lengths for authentication and encryption. For the high-security level (HSL), the key length (KL_{HSL}) is set according to $HSL_{Parameters}$, while for the low-security level (LSL), the key length (KL_{LSL}) is determined by $LSL\_Parameters$. Longer keys provide greater security but may need more computing power.

Key Refresh Rates: ETESLA enables nodes to select key refresh rates based on the security level. The refresh rate (RR) determines how often cryptographic keys are updated. For HSL, the refresh rate (RR_{HSL}) is set as per $HSL_{Parameters}$, and for LSL, it is determined by $LSL_{Parameters}$. Frequent key updates can enhance security, especially for critical data.

Key Pools: To manage keys efficiently, ETESLA maintains separate key pools for different security levels. Nodes utilize the appropriate key pool based on the security level it are operating under. For example, there is a Key Pool for HSL (KP_{HSL}) and a Key Pool for LSL (KP_{LSL}), each containing keys relevant to their respective security levels.

Data Classification: Nodes classify data into different security levels based on application requirements. A Data Classification Function (DCF) is used to determine the appropriate security level (SL_{Data}) for each data packet. This classification ensures that data receives the suitable level of protection.

Cross-Layer Integration: ETESLA can integrate with other MANET protocols, such as routing and quality of service (QoS) mechanisms. Security parameters can now be dynamically changed based on network conditions thanks to this integration. For instance, the refresh rates (RR_{HSL} andRR_{LSL}) may be modified in response to changing QoS metrics.

Localized Security Policies: Nodes can implement localized security policies based on their roles or positions within the network. A Security Policy Function (SPF) is used to define policies based on node characteristics, such as whether a node is a gateway or part of the network interior. The chosen security level (SL_{Node}) is determined by SPF.

Dynamic Adaptation: ETESLA supports dynamic adaptation of security settings in response to real-time network conditions. This means that security parameters, including refresh rates and key lengths, can be adjusted dynamically based on factors like network metrics. For example, RR_{HSL} can be adapted based on observed network behavior.

Algorithm for Enhanced TESLA

Step 1: Start the process.
Step 2: For every security level, specify the security settings.
Step 3: Define High Security Level Parameters denoted as HSL_P & Low Security Level Parameters denoted as LSL_P
Step 4: Make Key Length Selection based on the security level
Step 5: Key Length (KL_{HSL}) = $HSL_{Parameters}.KeyLength$ & Key Length (KL_{LSL}) = $LSL_{Parameters}.KeyLength$
Step 5: Determine key refresh rates based on security level
Step 6: For High Security Level, Refresh Rate (RR_{HSL}) = $HSL_{Parameters}.RefreshRate$
Step 7: For Low Security Level, Refresh Rate (RR_{LSL}) = $LSL_{Parameters}.RefreshRate$
Step 8: Maintain separate key pools for different security levels.
Step 9: Initialize Key Pool for HSL and LSL as HSL (KP_{HSL}) and LSL (KP_{LSL})
Step 10: Data Classification Function (DCF) = Classify (Data)
Step 11: Apply Security Level for Data (SL_{Data}) = DCF (Data)
Step 12: Adjust security parameters based on network conditions dapt RR_{HSL} and RR_{LSL}
Step 13: Implement Security Policy Function (SPF) =$DefinePolicy(NodeRole)$
Step 14: Apply node-specific security policies (SL_{Node}) = $SPF(NodeRole)$
Step 15: Dynamically adapt security settings Adjust RR_{HSL} and RR_{LSL} as $RR_{HSL} = DynamicAdaptation(NetworkMetrics)$
Step 16: Stop the process.

ETESLA's support for multiple security levels in MANETs provides flexibility in tailoring security measures to the specific needs of different types of data and communication. This customization ensures that critical data receives the highest level of protection while optimizing resource utilization in the dynamic and often resource-constrained MANET environment.

4. Experiment Results

4.1 Packet Delivery Ratio (PDR)

It is the proportion between the number of packets transmitted and received.

Table 1. Comparison Table of Packet Delivery Ratio (PDR)

No of Nodes	ECCHC	FSMR	Proposed ETESLA

100	75	71	85
200	78	75	90
300	80	75	92
400	83	77	94
500	85	79	97

The comparison table 1 of Packet Delivery Ratio (PDR) addressed the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 75 to 85 and 71 to 79 and proposed ETESLA values start from 85 to 97. The proposed gives the best result.

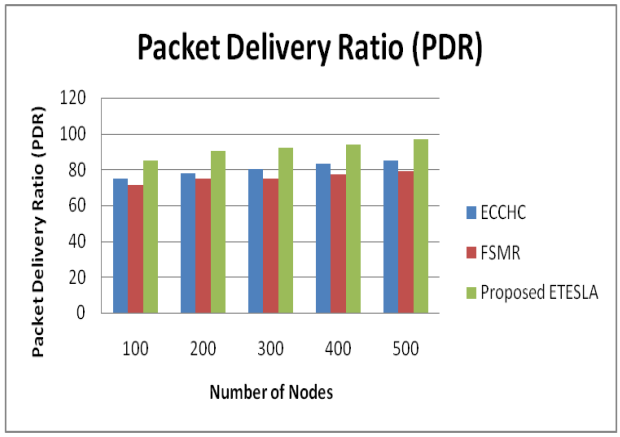

Figure 1 Comparison chart of Packet Delivery Ratio (PDR)

The figure 1 data Packet Delivery Ratio (PDR) describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Packet Delivery Ratio (PDR) in Y axis. The existing values start from 75 to 85 and 71 to 79 and proposed ETESLA values start from 85 to 97. The proposed gives the best result.

4.2 Throughput

It denotes that the number of packets successfully received by the receiver.

Table 2 Comparison Table of Throughput

No of Nodes	ECCHC	FSMR	Proposed ETESLA
100	60	63	70
200	64	66	74
300	66	68	77
400	67	73	79
500	70	77	82

The comparison table 2 of Throughput describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 60 to 70, 63 to 77 and the proposed ETESLA values start from 70 to 82. The proposed gives the best result.

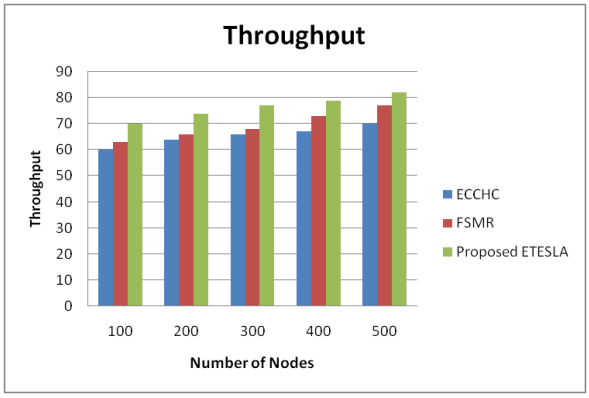

Figure 2 Comparison Chart of Throughput

The figure 2 data Throughput describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and throughput in Y axis. The existing values start from 60 to 70, 63 to 77 and the proposed ETESLA values start from 70 to 82. The proposed gives the best result.

6.4.3 Average Delay

Average Delay refers to the time it takes for a packet or data to travel from the source node to the destination node in a network

Table 3 Comparison Table of Average Delay

No of Nodes	ECCHC	FSMR	Proposed ETESLA
100	66	53	42
200	66	63	47
300	74	75	65
400	77	81	69
500	80	85	74

The comparison table 3 of Average Delay describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 66 to 80 and 53 to 85 and proposed ETESLA values start from 42 to 74. The proposed gives the best result.

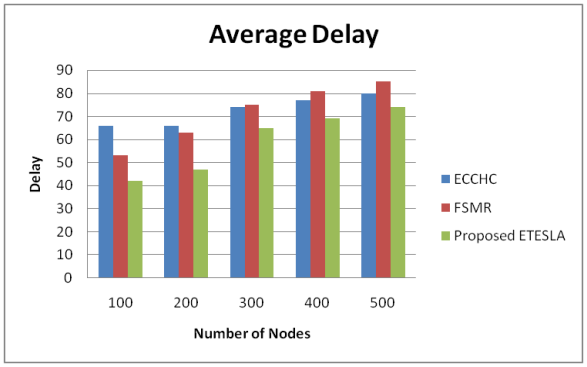

Figure 3 Comparison Table of Average Delay

The figure 3 Average Delay describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and the proposed method values are higher than the existing method

and No of Nodes in x axis and Average Delay in Y axis. The existing values start from 66 to 80 and 53 to 85 and proposed ETESLA values start from 42 to 74. The proposed gives the best result.

4.4 Remaining Energy

Remaining Energy refers to the amount of energy that is still available or remaining.

Table 4 Comparison Table of Remaining Energy

No of Nodes	ECCHC	FSMR	Proposed ETESLA
100	100	100	100
200	75	82	91
300	63	73	82
400	44	61	72
500	35	42	57

The table 4 comparison of Remaining Energy describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 100 to 35, 100 to 42 and proposed ETESLA values start from 100 to 57. The proposed gives the best result.

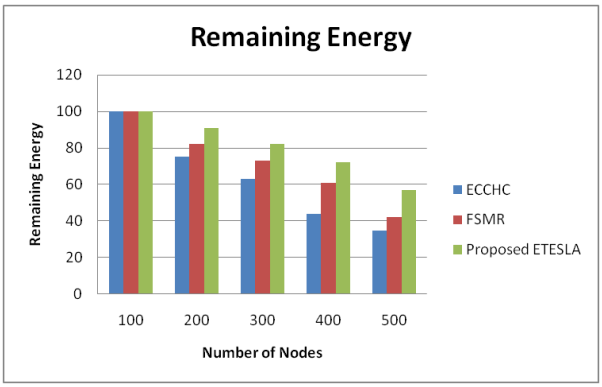

Figure 4 Comparison Chart of Remaining Energy

The figure 4 data Remaining Energy describes the different values of existing (ECCHC, FSMR) and proposed ETESLA. While comparing the existing and the proposed ETESLA method values are higher than the existing method No of Nodes in x axis and Remaining Energy in Y axis. The existing values start from 100 to 35, 100 to 42 and proposed ETESLA values start from 100 to 57. The proposed gives the best result.

5. Conclusion

In the realm of Mobile Ad Hoc Networks (MANETs), security authentication has been a persistent challenge. This research introduced a novel approach to address this challenge, utilizing the ETESLA-ACK protocol. By employing Authentication Tokens (AT) containing message details, expiration times, and digital signatures, nodes can securely authenticate each other. The proposed scheme enhances message integrity and relevance, while periodic key renewals and group key updates bolster overall network security. Simulations confirm the efficacy of this approach in fortifying MANET communications, making it a valuable contribution to the realm of MANET security.

References

[1] Almaiah MA, Dawahdeh Z, Almomani O, Alsaaidah A, Al-Khasawneh A, Khawatreh S. A new hybrid text encryption approach over mobile ad hoc network. Int. J. Electr. Comput. Eng. (IJECE). 2020 Dec; 10(6):6461-71.

[2] Brindha V, Karthikeyan T, Manimegalai P. Fuzzy enhanced secure multicast routing for improving authentication in MANET. Cluster computing. 2019 Jul; 22(Suppl 4):9615-23.

[3] Kaur N. A Review of Biometric based Authentication for MANET. In2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) 2018 Dec 20 (pp. 575-579). IEEE.

[4] Bondada P, Samanta D, Kaur M, Lee HN. Data security-based routing in MANETs using key management mechanism. Applied Sciences. 2022 Jan 20; 12(3):1041.

[5] Usha MS, Ravishankar KC. Implementation of trust-based novel approach for security enhancements in MANETs. SN Computer Science. 2021 Jul; 2(4):257.

[6] S. Liu, H. Xu and R. Zang, "An Improved Anonymous Authentication Scheme for Internet of Medical Things Based on Elliptic Curve Cryptography," 2023 5th International Conference on Natural Language Processing (ICNLP), Guangzhou, China, 2023, pp. 345-349, doi: 10.1109/ICNLP58431.2023.00069.

[7] R. Patan and R. M. Parizi, "Automatic Detection of API Access Control Vulnerabilities in Decentralized Web3 Applications," 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Athens, Greece, 2023, pp. 76-85, doi: 10.1109/DAPPS57946.2023.00019.

[8] B. Chatterjee, D. Das and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 2018, pp. 205-208, doi: 10.1109/HST.2018.8383916.

[9] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777334.

[10] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196-248, Firstquarter 2020, doi: 10.1109/COMST.2019.2933899.