Wireless Networks (2021) 27:893–907
https://doi.org/10.1007/s11276-019-02185-2

Efficient pre-authentication scheme for inter-ASN handover in high mobility MANET

M. Deva Priya[1] · Sengathir Janakiraman[2] · G. Sandhya[1] · G. Aishwaryalakshmi[3]

Published online: 15 November 2019

Abstract
Ensuring Quality of Service (QoS) and providing seamless connectivity are challenging in a mobile adhoc network. When Mobile Subscriber Station (MSS) moves between Access Service Network (ASNs), the authentication delay incurred during inter-ASN handover becomes a bottleneck. Pre-authentication of the MSSs at the target ASN (tASN) reduces the handover delay. Some existing pre-authentication schemes are prone to attacks. Modified EAP based Pre-authentication scheme using Improved ElGamal (MEPIE) proposed in this paper, modifies the existing Enhanced EAP based pre-Authentication scheme by using improved ElGamal digital signature and ElGamal encryption algorithm. To overcome the Denial of Service (DoS) and the replay attacks, MEPIE enhances ElGamal by using additional random variables. It outperforms the existing schemes in terms of Throughput, Packet Delivery Ratio (PDR), authentication delay, number of keys and Packet Loss Ratio (PLR) with negligible computation overhead.

Keywords Mobile ad hoc networks · Authentication · Cryptography · Digital signatures · Handover · DoS · Replay attacks

1 Introduction

Mobile Adhoc NETworks (MANETs) formed on demand are infrastructure-less and have no centralized control. There are various challenges including mobility and wide deployment of nodes, which makes it vulnerable to attacks. Further, resource constraint is another factor that plays a vital role in MANETs. Hence, the security mechanisms designed to safeguard them should be energy conservative.

Dropping of calls during mobility of a node from a Base Station (BS) or Access Service Network Gateway (ASN-GW) to another will affect incessant services and degrade performance. The nodes in a MANET should be authenticated to become a part of the network and the services therein. Mobile WiMAX (IEEE 802.16e) offers better QoS by supporting high data rate. In a highly mobile WiMAX based network, as nodes move between Gateways (GWs), they have to authenticate to enter into a new network. To support seamless service, the handover process should involve minimal time. Predominant challenges in handover include providing uninterrupted services, authentication, session recovery, supporting movement across dissimilar networks, provisioning of QoS and choosing proxy servers.

In a network, malicious nodes may make use of the message identity and the region of origin to gain access to the information shared between the ASN-GWs. Pre-authentication between the MSS and the Authentication Server (AuS) aids in circumventing the increased

✉ M. Deva Priya
m.devapriya@skct.edu.in

Sengathir Janakiraman
j.sengathir@gmail.com

G. Sandhya
sandhya.g@skct.edu.in

G. Aishwaryalakshmi
g.aishwaryalakshmi@skct.edu.in

[1] Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

[2] Department of Information Technology, CVR College of Engineering, Mangalpally, Vastunagar, Hyderabad, Telangana, India

[3] Department of Information Technology, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

authentication delay that interrupts the services and upsurges handover delay and packet loss [49].

When a MSS enters a network, communication parameters and other control information are negotiated with the BS [6]. As the MSSs must be authenticated to create a distinct digest, entry management messages are secured. Resources may be wasted if an intruder exploits RaNGeREQest (RNG-REQ) messages, arbitrarily changes some fields and sends multiple messages to the BS [44].

If an adversary sends more number of false authorization requests to the BS, increased amount of resources will be spent in proving the integrity of the certificate [28]. A BS with low computational resources becomes incompetent to handle invalid messages, leading to the success of Denial of Service (DoS) attack [30]. Trusted authorization is needed as guaranteeing reliability of messages is challenging [40]. Anybody with an appropriately positioned radio receiver can take hold of authorization messages, alter and forward it. Digital signatures ensure authenticity, integrity and prevent the sender from disclaiming having sent the message. Encryption ensures privacy.

In this paper, a pre-authentication scheme is propounded for MANETs. The existing Modified Extensible Authentication Protocol based Pre-authentication scheme using ElGamal (MEPE) involves ElGamal digital signatures. The proposed Modified EAP based Pre-authentication scheme using Improved ElGamal (MEPIE) uses improved ElGamal digital signatures and ElGamal encryption & decryption algorithms. It ensures security by involving insignificant amount of computational resources.

The main motivation for the proposed scheme is the demand to minimize the communication overhead and the authentication delay involved in ensuring security during inter-ASN handover in MANET.

The paper is structured as follows: Section 2 details the work done by various researchers related to authentication and pre-authentication in MANET. Section 3 describes about the security aspects of the proposed Improved EAP based Pre-Authentication Scheme. Section 4 shows the procedure of Authentication using MEPIE. Sections 5 and 6 depicts the results and conclusion respectively.

2 Related work

Authentication using Certificate Authority (CA) and Public Key Infrastructure (PKI) is essential to ensure security [19]. To ensure trustworthiness and easy accessibility in a distributed network, it is predominant to establish secure links with proper authentication.

2.1 Authentication

Among the many techniques propounded to provide authentication, Kerberos seems to be the elementary technology [32] proposed for wireless networks. It provides authentication based on passwords but do not overcome password guessing attacks. To overcome the delay incurred in Kerberos, Patidar et al. [38] have proposed Multi-level Security Authentication (MLSA) that supports resource sharing in MANET.

Hafslund et al. [13] have secured network access in hybrid MANET by providing authentication based on EAP [2] and RADIUS [1]. 802.11i supports only single hop communication.

Nodes should be verified by using an asymmetric key pair. Certificate Authorities (CAs) enable signing the packets digitally using a shared secret. Unreadable packets are discarded. This scheme provides point-to-point authentication and prevents replay attacks using unique timestamps [14, 16].

Ammayappan et al. [4] have proposed an integrated cryptographic scheme comprising of Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC). Mutual authentication and key management are done to ensure integrity of messages in one hop MANETs. Key storage and distribution are done to ensure secured data transmission. This decentralized scheme generates a shared secret key between collaborative nodes.

Larafa and Laurent-Maknavicius [26] have analyzed the behavior of neighboring nodes using game theory with whole information. The nodes involve less privacy loss and cost. Larafa and Laurent [25] have dealt with designing Authentication, Authorization, Accounting (AAA) infrastructures for access. In their former works, they have propounded a theoretical AAA framework, wherein nodes authenticate to several AAA servers and the communicating nodes check the legality of the node to grant access [26, 27]. Saxena et al. [43] have proposed an admission control technique that uses bivariate polynomials. Caballero-Gil and Hernández-Goya [5] have propounded a self-organized distributed authentication scheme for MANETs. It takes into account certain characteristics of MANET including imperfect protection, dynamic route changes and lack of structured hierarchy. The proposed Global Authentication Scheme for MANETs (GASMAN) is based on the Zero-Knowledge Proofs (ZKPs), a well-known cryptographic model [12]. Information related to security is not transmitted during the process of authentication.

Ali et al. [3] have proposed MANIPsec by modifying IPsec. They have focused on providing lightweight security, authentication and confidentiality for control and routing traffic. Network control traffic demands substantial

amount of resources in contrast to application driven traffic. Diffie and Hellman algorithm [9] provides one-way authentication against third party counterfeits [7]. There are chances for transmitter–receiver conflicts and is computationally expensive. Xingliang and Shilian [51] have used a Certificate Store server to issue the Diffie–Hellman public key to the nodes.

Sridevi and Rajaram [46] have proposed a scheme to deal with secure key distribution using EAP integrated Private Key Management version 2 (PKMv2). Keys are cached so as to reduce the authentication delay.

Effective Trusted Communication (ETC) proposed by Ruengsatra et al. [42] deals with routing and authentication to ensure trusted communication. Priana [39] has proposed trusted clustering and authenticated multicast for adhoc networks. Cluster heads communicate on behalf of clusters and the protocol uses the source's encrypted key to provide confidentiality. The agent verifies the nodes added to a network.

Though, several authors have proposed lightweight and energy efficient protocols, bilinear pairing makes the scheme expensive for energy constrained networks. To overcome this demerit, Kasra-Kermanshahi and Salleh [22] have propounded a public key authentication scheme using ECC instead of bilinear pairings.

Though Certificate-Less Public Key Cryptography (CL-PKC) offers less complex group key management as mentioned afore, there are schemes that rely on bilinear pairing, thus increasing the computation overhead. Xiaozhuo et al. [50] have proposed a Huffman-tree-based Pairing Free authenticated Certificate-Less Group Key Agreement Protocol (HPF-CLGKA) that aids in generating the group key. The protocol does not involve pairing and generation of signatures for authentication, thus reducing the computation overheads. The communication and control overheads are reduced by diminishing the negotiation rounds in the Huffman key tree.

Srividya and Ramesh [47] have proposed an authentication technique for emergency systems, in which biometric traits are used in the authentication of mobile users. Both physiological and behavioral biometrics traits involving finger photo recognition of a person are used by the proposed right shift algorithm. Kumar et al. [23] have used identity based symmetric key management scheme that involves ECC and bilinear pairing. Such schemes seem to be simple in contrast to PKI, as key management involves less memory. Ad hoc On-demand Distance Vector (AODV) is modified and the performance of ECC is compared with PARI/GP.

Pari et al. [37] have designed a Secure Hash Algorithm 1 (SHA-1) based secured model. Trust is determined based on the former experience and consents of nodes in the network. Message Authentication Codes (MAC) is constructed from cryptographic hash functions (SHA-256) for providing message authentication and ensuring data integrity in hybrid routing protocols [41]. Dilli and Reddy [10] have ensured security in routing using SHA3-256. Data integrity and authentication in Zone Routing Protocol (ZRP) are guaranteed through Hashed MAC (HMAC).

Hurley-Smith et al. [18] has developed Security Using Pre-Existing Routing for MANets (SUPERMAN) framework to perform authentication, access control and security. It focuses on issues related to routing and network layer security, while other protocols offer a choice in doing it. Nissar et al. [35] have enhanced AODV in terms of authentication by using digital signatures to circumvent attacks in routing. Hmouda and Li [15] have dealt with packet drops in the network. They have modified Enhanced Adaptive Acknowledgement (EAACK) protocol based on hybrid cryptography techniques like Data Encryption Standard (DES) and RSA as they efficiently perform block encryption and manage key ciphers respectively.

Suárez-Armas et al. [48] have developed Robotic MANET, wherein robots and Internet of Things (IoT) devices move to the anticipated location. In this decentralized approach, diverse security techniques are proposed to support authentication and encryption of information transmitted in the network. Identity-based Cryptography using Identity-Based Signcryption is employed to ensure secured communication.

2.2 Pre-authentication at the gateways

Pre-authentication minimizes handover delay and packet losses during authentication. Once the GW to which the mobile node should connect is identified, pre-authentication procedure can commence.

Jönsson et al. [21] have modified Mobile IPv4 (MIP4) to enable seamless movement of nodes across GWs by authenticating with a Foreign Agent (FA) located at the GW. This scheme supports only Mobility for IPv4 (MIP4). Pack and Choi [36] and Mishra et al. [31] have not permitted the transfer of control information through an AAA server. The keys are available at the GWs, and hence the AAA server is aware of the location of the GWs. This seems hectic as the mobile node should know the GWs to which it should pre-authenticate with. IEEE 802 LAN/MAN Standards Committee [20] and Dutta et al. [11] have introduced pre-authentication. The mobile node commences the process of authentication when it is likely to move to a new GW. Thus, authentication is completed before handover.

Housley and Aboba [17] have focused on secured transfer of control information from one GW to another, while Marin et al. [29] have concentrated on packet losses during inter-GW handover. As only authorized traffic is

permitted between GWs, the authentication delay is reduced. A utility-based optimal control is proposed for pre-authentication of mobile nodes.

2.2.1 EAP-Transport Layer Security (EAP-TLS)

EAP-Transport Layer Security (EAP-TLS) based mutual authentication is highly preferred by WiMAX forum. Mobile WiMAX guarantees security by using TLS protocol [28]. During handover between ASNs, distribution of Traffic Encryption Key (TEK) demands a complete EAP authentication. As Privacy Key Management (PKM) version 1 (PKMv1) supports one way authentication, it is susceptible to attacks. This challenge is overcome in PKM version 2 (PKMv2) [24] as it supports EAP based authentication between the BS and the MSS. Nevertheless, it is the user's responsibility to be responsive to counterfeit identifications. As presented by Simon et al. [45], EAP-TLS based authentication includes numerous rounds of public key operations. To begin with, the MSS forwards a request to the BS, which in turn sends it to the authenticator at the ASN.

2.2.2 EAP based pre-authentication

The EAP-based pre-authentication (EPA) [49] uses PKI. Initially, a MSS mutually authenticates with the home ASN (hASN), followed by pre-authentication with the neighboring ASNs (nASNs). As the nASNs have all the key related information shared by the MSS, a 3-way handshake with the nASNs would be adequate.

EPA comes with some drawbacks. As nonce is not employed to ensure message freshness, it is susceptible to DoS and replay attacks. As the MSS shares the key materials with all the nASNs including the ones that are not involved in communication, it becomes an overhead. Certificate forwarding and verification consumes more resources. A foe can claim that the hASN has forwarded a list containing neighbors and replay the same. Repeated pre-authentication interrupts normal operations by replaying authentication requests and responses. An opponent can forward a request to the nASNs through the hASN.

2.2.3 Enhanced EAP based pre-authentication scheme

Enhanced EAP-based Pre-authentication (EEP) scheme takes lesser amount of resources when compared to EPA [34]. It overcomes DoS and replay attacks. The centralized AuS uses information obtained from previous authentication. MAC is shared between the MSS and the home Base Station (hBS), while a secret key is shared between the ASN authenticator and the AuS. The AuS certificate can be indirectly obtained during the handshake between the AuS and the MSS. EEP uses RSA for encryption and signature generation.

EEP has some drawbacks. RSA is susceptible to attacks [33]. The message including Pre-Master Secret (PMS), nonce, Session IDentifier (SID) and identifier of the Mobile Subscriber Station (ID_{MSS}) is sent to the hBS. Only PMS is encrypted. The AuS forwards the unencrypted message (M') created by concatenating the SID, the Nonces (N_{AAA}, N_{MSS}) and the 'ID_{MSS}' to the MSS. In addition, the signatures are verified using only public keys. Random numbers are not involved.

3 Improved EAP based pre-authentication scheme

In this paper, Modified EAP based Pre-authentication scheme using Improved ElGamal (MEPIE) is propounded to overcome the challenges of EEP. It uses ElGamal encryption and decryption and improved ElGamal digital signature algorithms.

ElGamal based digital signature, a variant of ElGamal crypto scheme involves discrete logarithms. Key generation resembles ElGamal encryption, comprising of signing and verification steps.

$$e_2 = e_1^d \bmod p \tag{1}$$

where p—Prime (1024 bits), e_1, e_2—Integers, (e_1, e_2, p)—Public Key (PK), d—Private key, arbitrarily chosen in the range [1, p − 1], r—Random secret [GCD(r, p − 1) = 1]

Statement 1:

Let the signatures generated for message 'M' be 'S_1' and 'S_2', whereas 'V_1' and 'V_2' are the verifications. If $V_1 \equiv V_2$, 'M' is accepted.

$$S_1 = e_1^r \bmod p \tag{2}$$

$$S_2 = (M - dS_1)r^{-1} \bmod (p-1) \tag{3}$$

$$V_1 = e_1^M \bmod p \tag{4}$$

$$V_2 = e_2^{S_1} S_1^{S_2} \bmod p \tag{5}$$

Let 'p' and 'r' be prime and random numbers respectively. Appropriate measures are to be taken in ElGamal to prevent prediction of 'p' and 'r'.

'p' should be suitably large, capable of preventing the use of index-calculus methods. Similarly, to overcome Pohlig–Hellman digital logarithm attack, 'p − 1' should be divisible by a suitably large prime number 'q'.

Adversaries may use verification algorithms to accept signatures built without the sender's private key. Signatures can be forged by selecting a random value for 'r' and computing 'S_1'. As the computational complexity of Discrete Logarithm Problem (DLP) is high, the adversary has

to try hard to randomly select 'S_2'. For a large value of 'p', the probability of success is '$\frac{1}{p}$', which is insignificant.

Random choice of values of 'r' conceals the secret key (d). If hashing is not done, adversaries will attempt for forgery attacks.

Likewise, if 'S_1' is not checked, with a single signature of a sender, an adversary will attempt to sign messages he wishes to intercept. In ElGamal, for every encryption, different cipher texts are generated with close certainty. The length of the cipher text is double the size of plaintext. Key generation involves less time in contrast to encryption/decryption.

3.1 Improved ElGamal digital signature

In the proposed system, two random variables are used to generate message and signatures. Let the random variables be 'r_1' and 'r_2'.

Statement 2:

If 'M' is taken as

$$M = \left(dr_2^{-1}S_1 + r_1S_2\right) \bmod (p-1) \tag{6}$$

instead of

$$M = (dS_1 + rS_2) \bmod (p-1) \tag{7}$$

then, the signatures are given by,

$$S_1 = e_1^{r_1} \bmod p \tag{8}$$

$$S_2 = (M - dS_1)r_2^{-1} \bmod (p-1) \tag{9}$$

The verifications resemble ElGamal. It is difficult to find 'S_1' and 'd' as 'r_1' 'r_2' are used in 'S_1' and 'S_2' respectively. Some protocol failures prevalent in ElGamal are overcome in the improved ElGamal digital signature.

Statement 3:

In customary ElGamal, if the secret exponent 'r' is known, 'S_1' can be computed, thus enabling easy detection of 'd'.

The congruence is given by

$$dS_1 = (M - rS_2) \bmod (p-1) \tag{10}$$

Hence,

$$d = \frac{(M - rS_2) \bmod (p-1)}{S_1} \tag{11}$$

Substitute Eq. (3). The value of 'd' can be easily computed, if the values of 'r', 'S_1', 'M' are known.

As only one random variable 'r' is used, the system can be easily broken.

There are $N = GCD(S_1, p-1)$ solutions for 'd', where 'N' is definitely small.

By verifying Eq. (1), the precise value of secret exponent 'd' can be determined.

In the system propounded, Eq. (8) is verified. It is not feasible to determine 'd' from 'S_1'. The congruence is given by,

$$dr_2^{-1}S_1 = (M - r_1S_2) \bmod (p-1) \tag{12}$$

Hence,

$$d = \frac{(M - r_1S_2) \bmod (p-1)}{r_2^{-1}S_1} \tag{13}$$

Since 'r_1' and 'r_2' are used, the probability of finding them together is challenging. As 'S_2' involves 'r_2', even if 'r_1', 'S_1', 'M' are available, the system cannot be broken to find 'd'.

There are $N = GCD\left(r_2^{-1}S_1, p-1\right)$ possible solutions for 'd'. The secret key (d) cannot be determined by verifying,

$$e_2 = e_1^{dr_2^{-1}} \bmod p \tag{14}$$

As 'r_2' is used with 'd', it is challenging to verify Eq. (14) and determine the value of 'd'. The system's security is ensured as it is demanding to determine the randomly generated value of 'r_2'.

Statement 4:

In ElGamal digital signature, same value of 'r' can be applied to two dissimilar messages.

Let the messages be 'M_1' and 'M_2'.

If the same value of 'r' is used in 'S_1', it will remain unchanged.

Let the values of 'S_2' values be taken as 'α' and 'β'.

Then,

$$-dS_1 = (\alpha r - M_1) \bmod (p-1) \tag{15}$$

$$-dS_1 = (\beta r - M_2) \bmod (p-1) \tag{16}$$

Hence,

$$(\alpha r - M_1) \bmod (p-1) = (\beta r - M_2) \bmod (p-1) \tag{17}$$

$$(\alpha - \beta)r = (M_1 - M_2) \bmod (p-1) \tag{18}$$

$N = GCD(\alpha - \beta, p-1)$ is the promising number of solutions for 'd', where 'N' is usually small.

The exact value of 'r' can be determined by considering the solution that fulfills Eq. (2).

On determining 'r', 'd' can be determined similar to the former case and the system becomes unsafe.

In the proposed scheme,

$$-dr_2^{-1}S_1 = (\alpha r_1 - M_1) \bmod (p-1) \tag{19}$$

$$-dr_2^{-1}S_1 = (\beta r_1 - M_2) \bmod (p-1) \tag{20}$$

Hence,

$$(\alpha r_1 - M_1) \bmod (p-1) = (\beta r_1 - M_1) \bmod (p-1) \quad (21)$$

$$(\alpha - \beta) r_1 = (M_1 - M_2) \bmod (p-1) \quad (22)$$

$N = GCD(\alpha - \beta, p-1)$ is the possible number of solutions, where 'N' is generally small. Further, the exact value of 'r_1' can be determined by verifying the 'N' options to determine the solution that satisfies Eq. (8). Once 'r_1' is obtained, 'd' can be easily computed.

By verifying Eq. (14), exact value of 'd' can be found. As 'r_2' is used with 'd', as in the former case, the system cannot be broken. Even if 'r_1' is known, 'r_2' cannot be predicted at the same time.

Statement 5:

Thirdly, if 'M', 'S_1' and 'S_2' are selected simultaneously, there are chances for generating valid signatures.

To generate signatures, integers 'i' and 'j' less than '$p-1$' are to be selected such that GCD (j, $p-1$) = 1. The signatures are shown in Eqs. (23) and (24).

$$S_1 = e_1^i e_2^j \bmod p \quad (23)$$

$$S_2 = -S_1 j^{-1} \bmod (p-1) \quad (24)$$

The message is given by,

$$M = iS_2 \bmod (p-1) \quad (25)$$

As random variable is not involved in Eq. (1), the system can be cracked by using integers 'i' and 'j'.

In the propounded algorithm, 'S_2' depends on 'S_1', while 'S_1' is dependent on 'e_2'. 'e_2' involves the random variable 'r_2'. Signatures cannot be generated without the knowledge of random variables.

4 Authentication using MEPIE

Handover decision may be taken by MSS or the hBS. The ID of the MSS (ID_{MSS}) and the desired tASN (ID_{tASN}) are forwarded to the tBS by the hBS.

The tBS sends its willingness to accept the handover to the hBS. The tASN generates and forwards the KEY_REQuest (KEY_REQ) to the AuS. Similar to EAP-TLS key derivation, the AuS derives the Master Session Key (MSK) [45].

Pseudo-Random Functions (PRFs) are used in generating the master secret and key material [8] as shown below.

$$\begin{aligned} &Master_{Secret} = TLS\_PRF\_48 \\ &(PMS, Master\_Secret, N_{MSS} || N_{AAA} || ID_{tASN}) \end{aligned} \quad (26)$$

$$\begin{aligned} &Key\_Material = TLS\text{ - }PRF\quad\text{ - }128(Master\_Secret,'' \\ &client\,EAP\,encryption'', N_{MSS} \| N_{AAA} \| ID_{tASN}) \end{aligned} \quad (27)$$

$$MSK = Key\_Material\,(0,\,63) \quad (28)$$

Digital signatures in the proposed MEPIE are generated using improved ElGamal algorithm. In contrast to EEP, the DoS and replay attacks are overcome by using 2 random variables. MACs prevent an adversary from demanding that the message is from the hBS.

Table 1 shows the nomenclatures used.

As generating MACs is challenging, messages cannot be altered. As fake certificates and messages are dropped, resources are preserved. The SID correlates PREAUTH_REQs and PREAUTH_RSPs, thus averting replay attacks.

Nonces help in overcoming DoS attacks as the freshness of the message is ensured. PREAUTH_REQs and PREAUTH_RSPs cannot be replayed. The hASN identifies the request and disregards it.

Eavesdropping of the PMS is not feasible as it is encrypted using 'e_{AAA}'. As the signatures involve both the private and public keys of the sender, the impersonation attacks are overcome. The proposed system circumvents Man in the Middle (MITM) attack by using signatures, certificates and MAC.

The propounded authentication scheme comprises of the ensuing steps.

Table 1 Nomenclature in MEPIE

Notation	Description
PREAUTH_INIT, PREAUTH_REQ, PREAUTH_RSP	Pre-authentication Initiation, Request and Response
$CERT_{AAA}$ and ID_{MSS}	Certificate of AAA and ID of MSS
e_{MSS}, $e_{hBS}$and e_{AAA}	Public keys of MSS, hBS and AAA
d_{MSS}, $d_{hBS}$and d_{AAA}	Private keys of MSS, hBS and AAA
$ENC_{e_{MSS}}$, $ENC_{e_{hBS}}$and $ENC_{e_{AAA}}$	Encryption using public keys of MSS, hBS and AAA
$DEC_{d_{MSS}}$, $DEC_{d_{hBS}}$ and $DEC_{d_{AAA}}$	Decryption using private keys of MSS, hBS and AAA
N_{MSS} and N_{AAA}	Nonces of MSS and AAA
$S_1, S_2, S_1', S_2', V_1, V_2, V_1', V_2'$	Signatures and verifications
r_1, r_2	Random secrets

4.1 Mutual authentication and pre-authentication

Similar to EEP, the AuS and the MSS are mutually authenticated and the MSS is confident on the AuS and the hBS. An authentication code is shared between the hBS and the MSS. Similar to EEP, the hBS initiates pre-authentication. The hBS sends a PREAUTH_INIT message comprising of a distinct 16 bit SID, up-to-date and verified AuS certificate and the MAC to the MSS. SID is updated when hBS initiates fresh pre-authentication session with the same MSS.

hBS $\rightarrow$ **MSS**: PREAUTH_INIT
$=$ SID||CERT_AAA||MESSAGE AUTHENTICATION CODE

4.2 Securing against replay attacks and generating PREAUTH_REQ

The MSS assures freshness of the SID and the MAC. It also ensures that it is from the hBS. The MSS ensures that the messages are not replayed as the PMS and nonce (N_{MSS}) are generated at random.

MSS: Checks the SID & MAC and generates
PMS and a Nonce (N_{MSS})

The encrypted PMS, SID, fresh nonce (N_{MSS}), IDentity of the MSS (ID_{MSS}) and the signatures 'S_1' and 'S_2' are included in the PREAUTH_REQ that is forwarded to the hBS.

The PMS is encrypted using the PK of the AuS, while the SID, N_{MSS} and the ID_{MSS} are encrypted using the PK of hBS (e_{hBS}).

MSS $\rightarrow$ **hBS**: PREAUTH_REQ $=$ Y $||S_1||S_2$

$$Y = C||X \tag{29}$$

$$C = ENC_{e_{AAA}}(PMS) \tag{30}$$

$$K = SID\ ||N_{MSS}||ID_{MSS} \tag{31}$$

$$X = ENC_{e_{hBS}}(K) \tag{32}$$

The signatures that are forwarded to the hBS are generated using improved ElGamal digital signature. 'S_1' is based on 'r_1' and 'e_{MSS}'.

'S_2' is based on the message (M), 'S_1', 'd_{MSS}' and 'r_2'.

$$S_1 = e_{MSS}^{r_1} \bmod p \tag{33}$$

$$S_2 = (M\ - d_{MSS}S_1)r_2^{-1} \bmod (p-1) \tag{34}$$

$$M = \left(d_{MSS}r_2^{-1}S_1 + r_1S_2\right) \bmod (p-1) \tag{35}$$

4.3 Verification of request signatures at the hBS

To get 'K', the hBS decrypts 'X' using the private key of the hBS. The hBS verifies whether the generated PREAUTH_INIT message is similar to the nonce and the SID. It uses 'e_{MSS}' and 'e_{hBS}' to generate 'V_1' and 'V_2'. The PREAUTH_REQ is forwarded to the AuS through the hASN.

$$DEC_{d_{hBS}}(X) = K \tag{36}$$

Check K

$$V_1 = e_{MSS}^{M} \bmod p \tag{37}$$

$$V_2 = e_{hBS}^{S_1}S_1^{S_2} \bmod p \tag{38}$$

hBS $\rightarrow$ **hASN** $\rightarrow$ **AuS**: PREAUTH_REQ $= Y||S_1||S_2$

4.4 Verification of request signatures at the AuS

The AuS verifies the signatures of the PREAUTH_REQ using 'e_{MSS}' and 'e_{AAA}'. The freshness and the integrity of the messages are ensured using 'N_{MSS}'.

$$V_1' = e_{MSS}^{M} \bmod p \tag{39}$$

$$V_2' = e_{AAA}^{S_1}S_1^{S_2} \bmod p \tag{40}$$

Once the integrity of the message is ensured, AuS decrypts 'C' using 'd_{AAA}' to obtain the PMS. It decrypts 'X' to obtain 'K'.

The AuS keeps 'N_{MSS}' and produces 'N_{AAA}'. Message (M′) is generated using 'd_{AAA}', 'r_1', 'r_2' and S_1' and S_2'.

S_1' uses 'e_{AAA}', whereas S_2' uses 'd_{AAA}', 'r_2' and S_1'. The PREAUTH_RSP includes K′, S_1' and S_2'.

K′ is built from SID, 'N_{AAA}', 'N_{MSS}' and 'ID_{MSS}'. The PREAUTH_RSP from the ASN is forwarded to the hBS through the hASN.

$$DEC_{d_{AAA}}(C) = PMS \tag{41}$$

$$DEC_{d_{AAA}}(X) = K \tag{42}$$

$$M' = \left(d_{AAA}r_2^{-1}S_1 + r_1S_2\right) \bmod (p-1) \tag{43}$$

$$S_1' = e_{AAA}^{r_1} \bmod p \tag{44}$$

$$S_2' = \left(M' - d_{AAA}\ S_1'\right)r_2^{-1} \bmod (p-1) \tag{45}$$

$$K' = SID||N_{AAA}||N_{MSS}||ID_{MSS} \tag{46}$$

AuS $\rightarrow$ **hASN** $\rightarrow$ **hBS**: PREAUTH_RSP $= K'||S_1'||S_2'$

4.5 Verification of response signatures at the hBS

The hBS verifies the SID, 'N_{AAA}', 'N_{MSS}' and 'ID_{MSS}'. The PREAUTH_RSP is verified using 'e_{AAA}' and 'e_{hBS}'.

K′ is encrypted using 'e_{MSS}'. The response is forwarded to the MSS.

Check K′

$$V_1' = e_{AAA}^{M\prime} \bmod p \tag{47}$$

$$V_2' = e_{hBS}^{S_1'} S_1'^{S_2'} \bmod p \tag{48}$$

$$Y' = ENC_{e_{MSS}}(K') \tag{49}$$

hBS → **MSS**: PREAUTH_RSP = $Y'||S_1'||S_2'$

4.6 Verification of response signatures at the MSS

The MSS ensures that the response and the request match. It stores the value of 'N_{AAA}'. The response is verified using 'e_{AAA}' and 'e_{MSS}'. By decrypting Y′ using 'd_{MSS}', the SID, Nonces (N_{AAA} and N_{MSS}) and 'ID_{MSS}' are obtained.

$$DEC_{d_{MSS}}(Y') = K' \tag{50}$$

$$V_1' = e_{AAA}^{M\prime} \bmod p \tag{51}$$

$$V_2' = e_{MSS}^{S_1'} S_1'^{S_2'} \bmod p \tag{52}$$

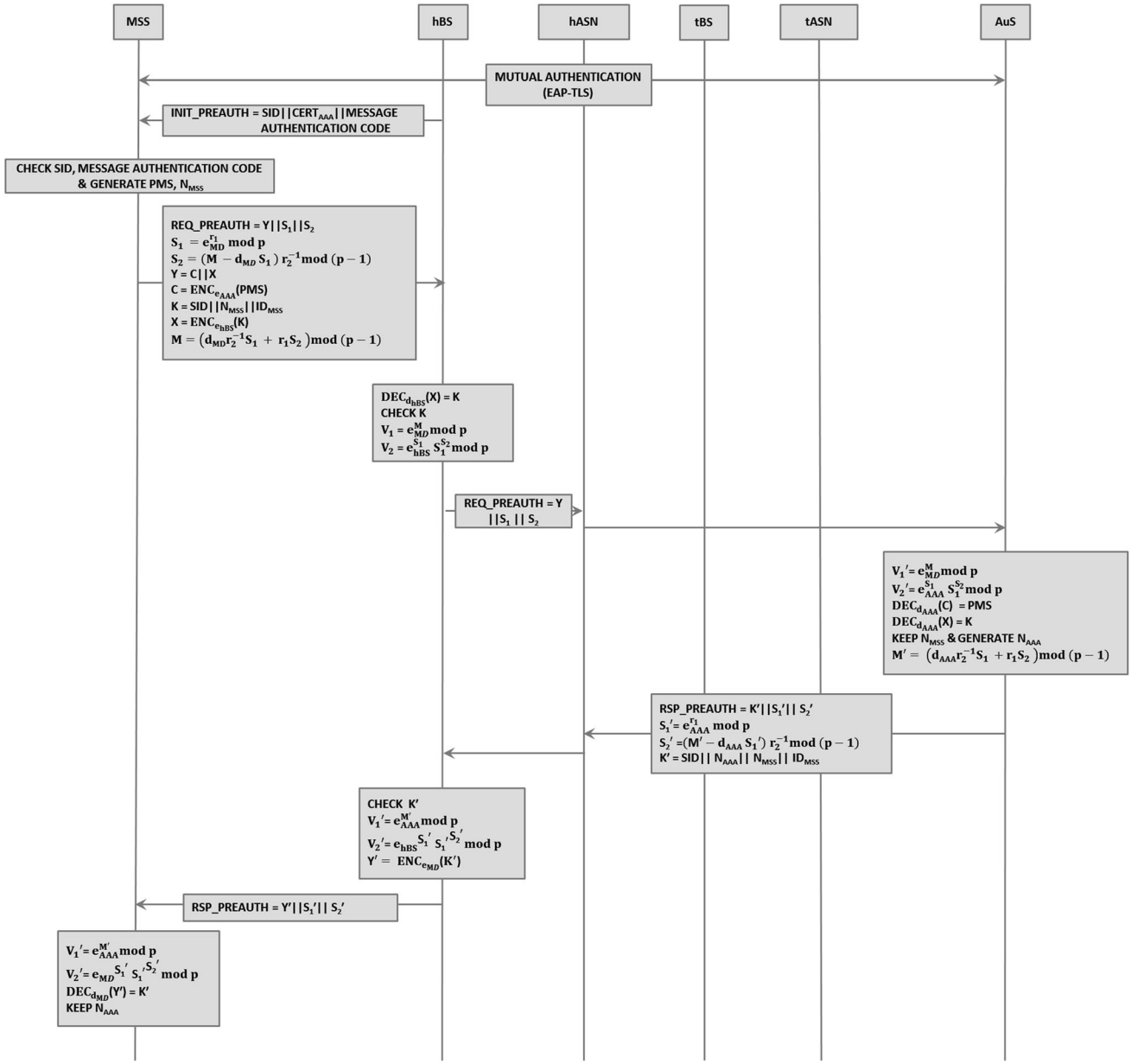

Fig. 1 MEPIE

Figure 1 shows the pre-authentication process of MEPIE. Both the signatures and the verifications are capable of withstanding attacks. They are generated using private & public keys, and two random variables. Further, encryption of the management messages shared between the MSS and the hBS complements to the system security.

5 Results and discussion

The performance of the EEP, MEPE and MEPIE schemes are evaluated and investigated using simulation experiments conducted using network simulator ns-2. In the simulation process, EEP is enhanced by generating digital signatures based on the inclusion of MEPE and MEPIE. In the MEPE scheme, signatures are generated using ElGamal and in the MEPIE, modified ElGamal is used for signature generation. The simulation setup and its associated parameters considered for achieving the simulation of the EEP, MEPE and MEPIE schemes are presented in Table 2.

The simulation experiments of EEP, MEPE and MEPIE schemes are evaluated in twofolds. In the first fold, EEP, MEPE and MEPIE schemes are evaluated in terms of Throughput, Packet Delivery Ratio (PDR), number of keys, Authentication Delay and Packet Loss Ratio (PLR) involving negligible Computation Overhead with respect to increasing Mobile Subscriber Stations (MSSs). In the second fold of investigation, EEP, MEPE and MEPIE schemes are evaluated with respect to increasing number of Malicious Stations.

Table 2 Simulation Parameters

Parameter	Value
MAC protocol	IEEE 802.16e
Encryption and decryption time	5 ms
Computing and verifying time	2 ms
Simulation time	500 s
Routing protocol	DSDV
Modulation scheme	OFDM_QPSK
Queue length	50
Queue type	Drop Tail/WFQ
Bandwidth	50 Mbps
Packet size	1024 bytes
Transmission range	250–400 m
Number of MSSs	100
Speed	1–40 m s^{-1}
Simulation time	80 s

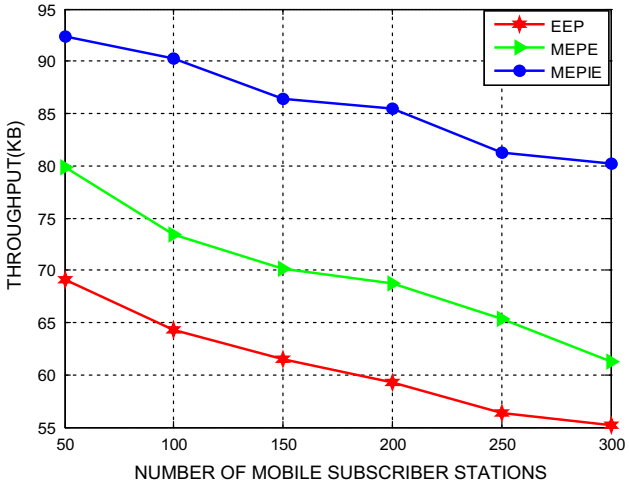

Fig. 2 Throughput of the proposed MEPIE and benchmarked MEPE and EEP for varying number of Mobile Subscriber Stations

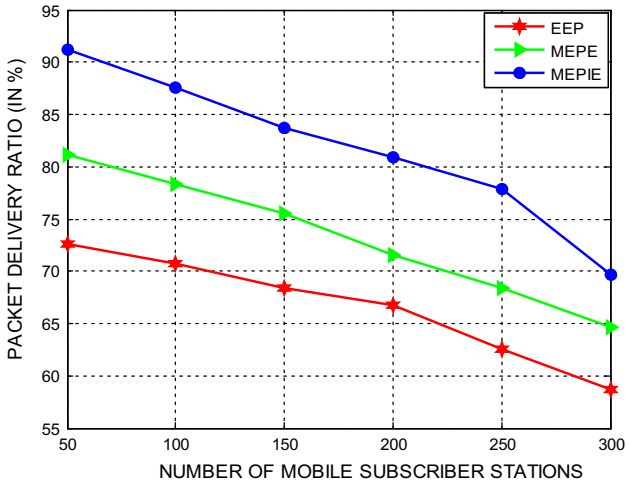

Fig. 3 Packet Delivery Ratio of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of Mobile Subscriber Stations

5.1 Performance evaluation based on the number of Mobile Subscriber Stations (MSSs)

In this investigation, the potential of EEP, MEPE and MEPIE schemes are evaluated and explored using Throughput, Packet Delivery Ratio (PDR), number of keys, Authentication Delay, Packet Loss Ratio (PLR) and Computation Overhead with respect to increasing number of MSSs.

Figures 2 and 3 demonstrate the Throughput and PDR of EEP, MEPE and MEPIE schemes for varying number of MSSs. The Throughput and PDR of MEPIE for varying

number of MSSs is determined to be excellent over the EEP and MEPE schemes, since it incorporates the concept of digital signatures for preventing DoS and replay attacks based on two random variables. These two variables used in MEPIE play an anchor role, such that MACs prevent an adversary from demanding the message to be generated from the hBS.

The Throughput of MEPIE for varying number of MSSs is identified to be improved by 32.3% and 23.2% in contrast to the EEP and MEPE schemes. Similarly, the PDR of the MEPIE for varying number of MSSs is identified to be improved by 22.8% and 11.7% when compared to the EEP and MEPE schemes.

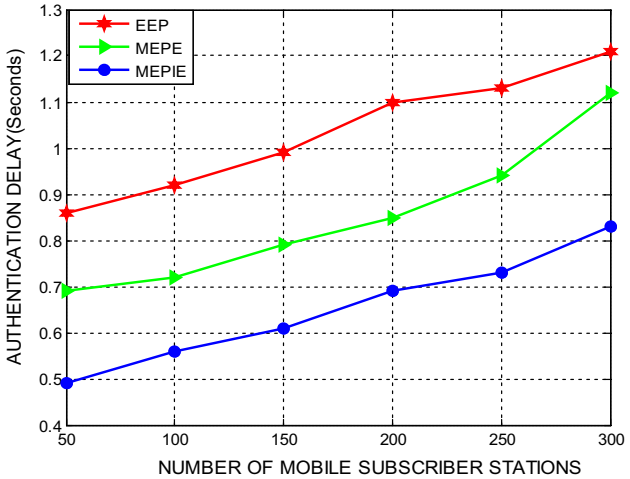

Fig. 4 Authentication delay of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of Mobile Subscriber Stations

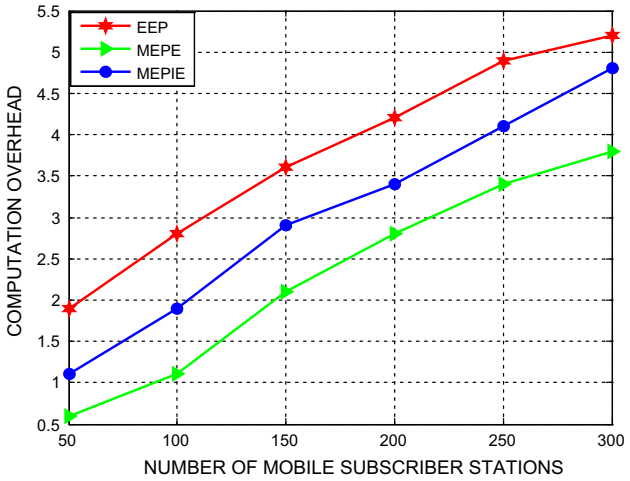

Fig. 5 Computation overhead of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of Mobile Subscriber Stations

Figures 4 and 5 portray the Authentication delay and Computation overhead of the EEP, MEPE and MEPIE schemes for varying number of MSSs. Since MEPIE uses the merits of modified ElGamal for signature generation, the authentication delay of MEPIE is better than the EEP and MEPE schemes.

The Authentication delay of MEPIE for varying number of MSSs is confirmed to be minimized by 42.9% and 28.6% when compared to EEP and MEPE schemes as it prevents attackers from gaining information and unnecessary computation. The Computation overhead involved in the implementation of MEPIE for varying number of MSSs is identified to be 31.9% more and 24.2% less when compared to the EEP and MEPE schemes.

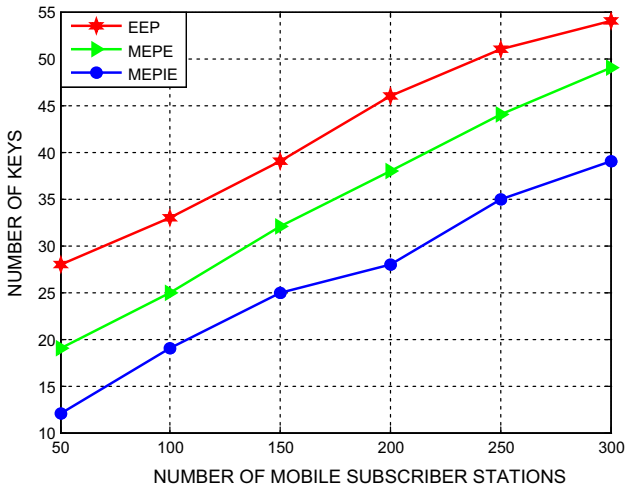

Fig. 6 Number of keys utilized by the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of Mobile Subscriber Stations

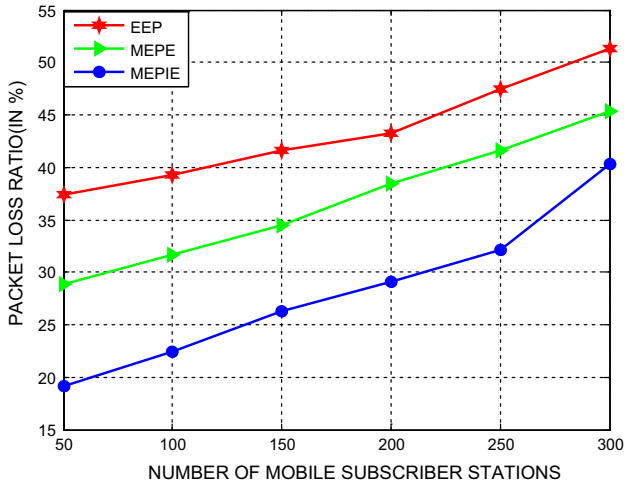

Fig. 7 Packet Loss Ratio of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of Mobile Subscriber Stations

Figures 6 and 7 depict the Number of keys utilized and Packet Loss Ratio (PLR) incurred during the implementation of the EEP, MEPE and MEPIE schemes for varying number of MSSs.

The number of keys utilized by MEPIE for varying number of MSSs is proved to be comparatively reduced over the EEP and MEPE schemes, since it is capable in establishing and facilitating reliable authentication process based on the merits of modified ElGamal for signature generation. Thus, the number of keys utilized by MEPIE for varying number of MSSs is confirmed to be minimized by 58.9% and 31.2%, when compared to the EEP and MEPE schemes. Similarly, the PLR of MEPIE for varying number of MSSs is also identified to be reduced by 53.8% and 30.3% in contrast to the EEP and MEPE schemes.

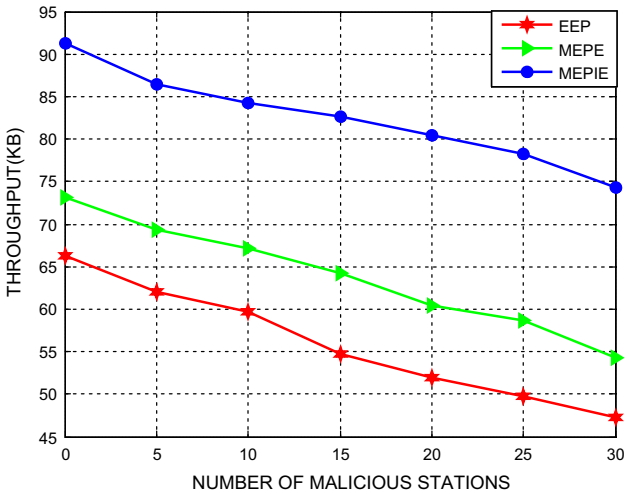

Fig. 8 Throughput of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of malicious stations

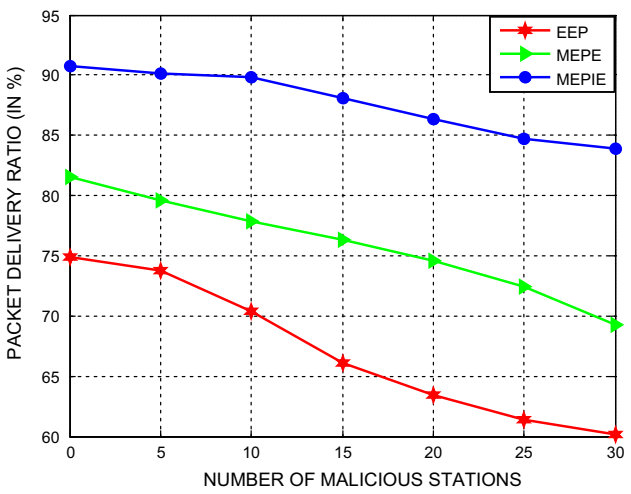

Fig. 9 Packet Delivery Ratio of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of malicious stations

5.2 Performance evaluation based on the number of malicious stations

In this investigation, the potential of the EEP, MEPE and MEPIE schemes are evaluated and explored in terms of Throughput, Packet Delivery Ratio (PDR), number of keys, Authentication Delay, Packet Loss Ratio (PLR) and Computation Overhead with respect to increasing malicious stations.

Figures 8 and 9 show the Throughput and PDR of the EEP, MEPE and MEPIE schemes for varying number of malicious stations. The Throughput and PDR of MEPIE under varying number of malicious stations is identified to be excellent over the EEP and MEPE schemes, as the

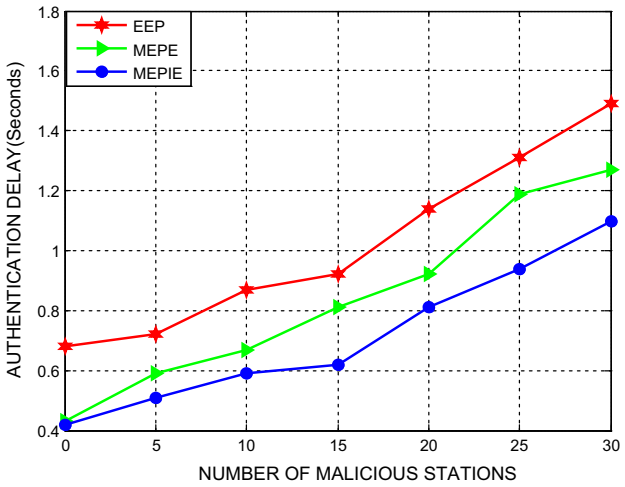

Fig. 10 Authentication delay of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of malicious stations

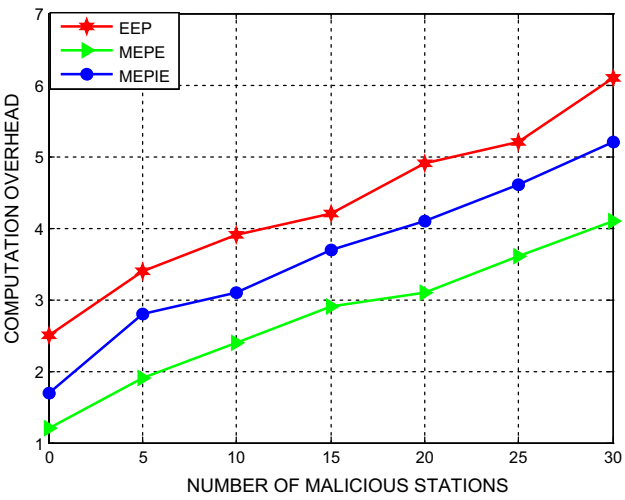

Fig. 11 Computation overhead of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of malicious stations

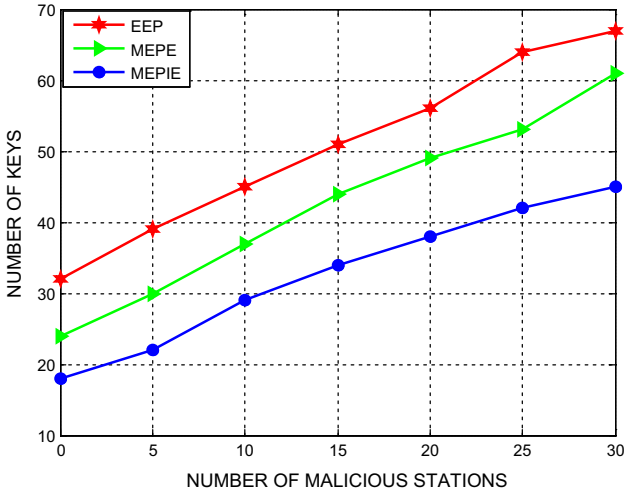

Fig. 12 Number of keys utilized by the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of malicious stations

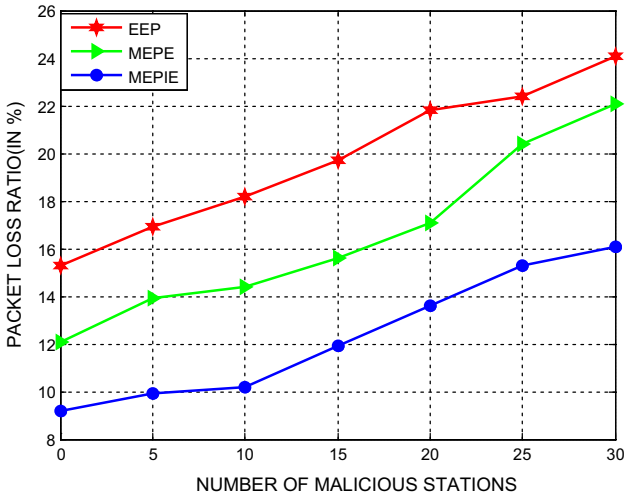

Fig. 13 Packet Loss Ratio of the proposed MEPIE and benchmarked MEPE and EEP schemes for varying number of malicious stations

malicious stations are circumvented based on mutual authentication process and unnecessary exchange of keys.

The Throughput of MEPIE for varying number of malicious stations is identified to be improved by 47.3% and 29.1%, in contrast to the EEP and MEPE schemes.

Similarly, the PDR of the MEPIE for varying number of malicious stations is identified to be improved by 30.5% and 15.5%, when compared to the EEP and MEPE schemes.

Figures 10 and 11 portray the Authentication delay and Computation overhead of EEP, MEPE and MEPIE schemes for varying number of malicious stations.

The Authentication delay of MEPIE is identified over the EEP and MEPE schemes, since it reduces the delay incurred in authentication by involving reduced number of keys.

Thus, the Authentication delay of the MEPIE for varying number of malicious stations is confirmed to be minimized by 43% and 14.3% in contrast to the EEP and MEPE schemes. Similarly, the Computation overhead involved in the implementation of MEPIE is considered to be 19.4% less than EEP and 33.3% more than MEPE schemes.

Moreover, Figs. 12 and 13 depict the number of keys utilized and Packet Loss Ratio (PLR) incurred during the implementation of the EEP, MEPE and MEPIE schemes for varying number of malicious stations. The number of keys utilized by MEPIE is identified to be phenomenally reduced on par with EEP and MEPE schemes, since it uses the merits of modified ElGamal for signature generation. Thus, the number of keys utilized by the MEPIE is confirmed to be minimized by 55.2% and 30.7% in contrast to the EEP and MEPE schemes.

Similarly, the PLR of MEPIE is identified to be reduced by 61% and 34.1% when compared to the EEP and MEPE schemes.

The results observed from Tables 3 and 4, clearly aids in realizing the time incurred by MEPIE, MEPE and EEP for

Table 3 Performance based on Number of Mobile Subscriber Stations

Time (ms)	Schemes	Number of Mobile Subscriber Stations (MSSs)					
		50	100	150	200	250	300
Key generation	EEP	38.42	57.71	78.42	97.81	121.62	176.43
	MEPE	18.31	24.56	32.91	49.72	61.94	70.95
	MEPIE	27.31	34.82	47.21	59.31	73.64	89.23
Signature generation	EEP	43.72	57.41	79.83	112.62	146.23	165.19
	MEPE	38.42	47.19	59.69	75.21	92.89	121.04
	MEPIE	41.42	50.32	62.70	81.35	97.43	132.09
Signature verification	EEP	18.32	29.72	43.67	56.81	71.32	84.19
	MEPE	11.51	18.02	29.82	41.05	56.49	64.32
	MEPIE	19.47	24.37	36.41	47.95	65.74	72.73

Table 4 Performance based on Number of Malicious Subscriber Stations

Time (ms)	Schemes	Number of Malicious Subscriber Stations					
		5	10	15	20	25	30
Key generation	EEP	4.93	7.07	8.98	11.83	16.54	22.35
	MEPE	3.52	4.26	5.59	7.5	9.4	9.91
	MEPIE	3.69	4.89	6.59	7.99	10.98	13.92
Signature generation	EEP	6.4	6.99	9.99	14.99	18.09	20.65
	MEPE	5.61	6.58	7.52	10.48	12.79	15.05
	MEPIE	5.81	6.71	7.72	12.52	15.91	19.97
Signature verification	EEP	2.77	4.38	5.72	8.01	8.62	11.49
	MEPE	2.23	3.5	3.7	5.54	6.6	7.98
	MEPIE	2.71	4.13	4.6	7.06	8.19	10.38

key generation, signature generation and signature verification based on the number of MSSs and number of malicious subscriber stations. These results portray the predominance of MEPIE over the compared MEPE and EEP schemes, since the detection rate of attacks, computation overhead and compromisation of the network by the attackers are potentially reduced.

6 Conclusion

The proposed Modified EAP based Pre-authentication scheme using Improved ElGamal (MEPIE) overcomes the MITM, replay, DoS and impersonation attacks in MANETs. The proposed mechanism based on the improved ElGamal addresses the inadequacies of ElGamal digital signatures and yields better results. From the results, it is evident that it outperforms the existing Enhanced EAP based Pre-Authentication (EEP) and the Modified EAP based Pre-authentication scheme using ElGamal (MEPE). The Mobile Subscriber Stations (MSSs) receive unhindered services as the delay incurred during authentication is reduced to a greater extent.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Aboba, B., & Calhoun, P. (2003). *RADIUS support for EAP*. IETF: Request for Comments.
2. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (2004). *Extensible authentication protocol (EAP)*, No. RFC 3748.
3. Ali, K. N., Basheeruddin, M., Moinuddin, S. K., & Lakkars, R. (2010). Manipsec-ipsec in mobile ad-hoc networks. In *Proceedings of 3rd IEEE international conference on computer science and information technology* (vol. 1, pp. 635–639).
4. Ammayappan, K., Sastry, V. N., & Negi, A. (2009). Authentication and dynamic key management protocol based on certified tokens for MANETs. In *IEEE global mobile congress* (pp. 1–6).
5. Caballero-Gil, P., & Hernández-Goya, C. (2009). Self-organized authentication in mobile ad hoc networks. *Journal of Communications and Networks, 11*(5), 509–517.
6. Chee, J., & Teo, M. (2011). Improving security in the IEEE 802.16 Standards. In *Proceedings of the 8th international conference on information technology: New generations* (pp. 408–412).
7. Dahshan, H., & Irvine, J. (2008). Authenticated symmetric key distribution for mobile ad hoc networks. In *Proceedings of the 5th IEEE international conference on mobile ad hoc and sensor systems* (pp. 847–852).
8. Dierks, T., & Rescorla, E. (2006). *The transport layer security (TLS) protocol Version 1.1, RFC 4346*.
9. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.
10. Dilli, R., & Reddy, P. C. S. (2016). Implementation of security features in MANETs using SHA-3 standard algorithm. In *Proceedings of the IEEE international conference on computation system and information technology for sustainable solutions* (pp. 455–458).
11. Dutta, A., Zhang, T., Ohba, Y., Taniuchi, K., & Schulzrinne, H. (2005). MPA assisted optimized proactive handoff scheme. In *Proceedings of the 2nd IEEE annual international conference on mobile and ubiquitous systems: Networking and services* (pp. 155–165).
12. Goldreich, O., Micali, S., & Wigderson, A. (1986). How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design. In *Proceedings of the conference on the theory and application of cryptographic techniques* (pp. 171–185). Berlin, Heidelberg: Springer.
13. Hafslund, A., Andersson, J., & AS, T. N. (2005). 2-Level authentication mechanism in an internet connected MANET. In *Proceedings of the 6th scandinavian workshop on wireless ad hoc networks, Johannesberg Estate*.
14. Hafslund, A., Tønnesen, A., Rotvik, R. B., Andersson, J., & Kure, Ø. (2004). Secure extension to the OLSR protocol. In *OLSR interop and workshop* (p. 1004).
15. Hmouda, E., & Li, W. (2018). Detection and prevention of attacks in MANETs by improving the EAACK protocol. In *Proceedings of the IEEE southeast conference* (pp. 1–7).
16. Hong, F., Hong, L., & Fu, C. (2005). Secure OLSR. In *Proceedings of the 19th IEEE international conference on advanced*

information networking and applications, AINA 2005 (vol. 1, No. 713-718).
17. Housley, R., & Aboba, B. (2006). *Guidance for AAA key management*. Draft-housley-aaa-key-mgmt-06, IETF Internet Draft.
18. Hurley-Smith, D., Wetherall, J., & Adekunle, A. (2017). SUPERMAN: Security using pre-existing routing for mobile ad hoc networks. *IEEE Transactions on Mobile Computing, 16*(10), 2927–2940.
19. Hwu, J. S., Chen, R. J., & Lin, Y. B. (2006). An efficient identity-based cryptosystem for end-to-end mobile security. *IEEE Transactions on Wireless Communications, 5*(9), 2586–2593.
20. IEEE 802 LAN/MAN Standards Committee. (1999). *Wireless LAN medium access control MAC and physical layer (PHY) specifications: Spectrum and transmit power management extensions in the 5GHZ Band in Europe, draft supplement to IEEE Standard* (p. 802).
21. Jönsson, U., Alriksson, F., Larsson, T., Johansson, P., & Maguire Jr., G. Q. (2000). MIPMANET: Mobile IP for mobile ad hoc networks. In *Proceedings of the 1st ACM international symposium on mobile ad hoc networking and computing* (pp. 75–85).
22. Kasra-Kermanshahi, S., & Salleh, M. (2015) A novel authentication scheme for mobile environments in the context of elliptic curve cryptography. In *Proceedings of the IEEE international conference on computer, communications, and control technology* (pp. 506–510).
23. Kumar, K. M. M., Sunitha, N. R., Mathew, R., Veerayya, M., & Vijendra, C. (2016). Secure ad-hoc on-demand distance vector routing using identity based symmetric key management. In *Proceedings of the IEEE international conference on wireless communications, signal processing and networking* (pp. 1075–1081).
24. Kolias, C., Kambourakis, G., & Gritzalis, S. (2013). Attacks and countermeasures on 802.16: analysis and assessment. *IEEE Communications Surveys and Tutorials, 15*(1), 487–514.
25. Larafa, S., & Laurent, M. (2010). Authentication protocol runtime evaluation in distributed AAA framework for mobile ad-hoc networks. In *Proceedings of the IEEE international conference on wireless communications, networking and information security* (pp. 277–281).
26. Larafa, S., & Laurent-Maknavicius, M. (2009). Protocols for distributed AAA framework in mobile ad-hoc networks. In *Proceedings of the workshop on mobile and wireless networks security* (pp. 75–86).
27. Larafa, S., Laurent-Maknavicius, M., & Chaouchi, H. (2008). Light and distributed AAA scheme for mobile ad-hoc networks. In *Proceedings of the 1st workshop on security of autonomous and spontaneous networks* (pp. 93–103).
28. Liu, D. Q., & Coslow, M. (2008). Extensible Authentication protocols for IEEE Standards 802.11 and 802.16. In *Proceedings of the ACM international conference on mobile technology, applications and systems*.
29. Marin, R., Ruiz, P. M., Ros, F. J., Martinez, J. A., & Gomez, A. F. (2007). Pre-authentication based enhancement for access control in hybrid MANETs. In *Proceedings of the 12th IEEE symposium on computers and communications* (pp. 595–600).
30. Maru, S., & Brown, T. X. (2008). Denial of service vulnerabilities in the 802.16 protocol. In *Proceedings of the 4th ACM annual international conference on wireless internet*.
31. Mishra, A., Shin, M. H., Petroni, N. L., Clancy, T. C., & Arbaugh, W. A. (2004). Proactive key distribution using neighbor graphs. *IEEE Wireless Communications, 11*(1), 26–36.
32. Neuman, B. C., & Ts'o, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications Magazine, 32*(9), 33–38.
33. Nguyen, T. D., Nguyen, T. D., & Tran, L. D. (2013). Attacks on low private exponent RSA: An experimental study. In *Proceedings of the 13th international conference on computational science and its applications* (pp. 162–165).
34. Nguyen, T. N., & Ma, M. (2012). Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks. *IEEE Transactions on Wireless Communications, 11*(6), 2173–2181.
35. Nissar, N., Naja, N., & Jamali, A. (2017). Lightweight authentication-based scheme for AODV in ad-hoc networks. In *Proceedings of the IEEE international conference on wireless technologies, embedded and intelligent systems* (pp. 1–6).
36. Pack, S., & Choi, Y. (2002). *Fast inter-AP handoff using predictive authentication scheme in a public wireless LAN, networks* (pp. 15–26).
37. Pari, S. N., Jayapal, S., & Duraisamy, S. (2012). A trust system in MANET with secure key authentication mechanism. In *Proceedings of the IEEE international conference on recent trends in information technology* (pp. 261–265).
38. Patidar, M., Sharma, M. K., & Bunglowala, A. (2014). Multilevel authentication for resource allotment in MANET. In *Proceedings of the IEEE conference on IT in business, industry and government* (pp. 1–4).
39. Priana, M. E. (2014). Trust based clustering and secure authentication for multicast in ad-hoc network. *International Journal of Computer Applications*, *108*(19), 54–63.
40. Qayyum, J., Lal, M., Khan, F., & Imad, M. (2011). Survey and assessment of WiMAX, its security threats and their solutions. *International Journal of Video and Image Processing and Network Security, 11*(3), 36–47.
41. Ravilla, D., & Putta, C. S. R. (2015). Implementation of HMAC-SHA256 algorithm for hybrid routing protocols in MANETs. In *Proceedings of the IEEE international conference on electronic design, computer networks and automated verification* (pp. 154–159).
42. Ruengsatra, T., Nakorn, K. N., Rojviboonchai, K., & Piromsopa, K. (2014). ETC: Effective trustworthy communication with two-mode authentication for disaster recovery. In *Proceedings of the 10th IEEE international conference on information assurance and security* (pp. 12–17).
43. Saxena, N., Tsudik, G., & Yi, J. H. (2009). Efficient node admission and certificateless secure communication in short-lived MANETs. *IEEE Transactions on Parallel and Distributed Systems, 20*(2), 158–170.
44. Shojaee, M., Movahhedinia, N., & Ladani, B. T. (2010). Traffic analysis for WiMAX network under DDoS attack. In *Proceedings of the 2nd Pacific-Asia conference on circuits, communications and system* (vol. 1, pp. 279–283).
45. Simon, D., Aboba, B., & Hurst, R. (2010). *The EAP-TLS Authentication Protocol, RFC 5216*.
46. Sridevi, B., & Rajaram, S. (2012). PKMv2–EAP authentication cost reduction of mobile WiMAX network entry process by the proposed key caching mechanisms. *International Journal of Mobile Network Design and Innovation, 4*(2), 65–75.
47. Srividya, R., & Ramesh, B. (2015). Design of biometric authentication technique for MANET based emergency response system. In *Proceedings of the IEEE international conference on electrical, computer and communication technologies* (pp. 1–5).
48. Suárez-Armas, J., Caballero-Gil, C., Rivero-García, A., & Caballero-Gil, P. (2018). Authentication and encryption for a robotic ad hoc network using identity-based cryptography. In *Proceedings of the 4th IEEE international conference on big data innovations and applications (innovate-data)* (pp. 71–76).
49. Sun, H. M., Lin, Y. H., Chen, S. M., & Shen, Y. C. (2007). Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks. In *Proceedings of the IEEE region 10 conference* (pp. 1–4).

50. Xiaozhuo, G., Zhenhuan, C., & Yongming, W. (2015). How to get group key efficiently in mobile ad hoc networks? In *Proceedings of the IEEE military communications conference* (pp. 1009–1014).
51. Xingliang, Z., & Shilian, X. (2012). A new authentication scheme for wireless ad hoc network. In *Proceedings of the IEEE international conference on information management, innovation management and industrial engineering* (vol. 2, pp. 312–315).

M. Deva Priya is currently working as Associate Professor in the Department of Computer Science and Engineering at Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India. She received her Master's degree in the year 2007 and her Ph.D. degree in the year 2015 from Anna University, Chennai, Tamilnadu, India. She has 12.5 years of teaching experience. Her research interests include Wireless and IoT Networks. She has published more than 45 papers in reputed Journals and Conferences. She is a life member of ISTE, ISRD, member in IAENG and Senior Member in UACEE.

Sengathir Janakiraman is currently working as an Associate Professor in the Department of Information Technology at CVR College of Engineering, Mangalpally, Telangana, India. He has received his B.Tech. degree in Computer Science and Engineering, M.Tech. degree in Information security and Ph.D. degree in Mobile ad hoc Networks from Pondicherry Engineering College, Pondicherry University, Puducherry, India. He is the recipient of the Pondicherry University Gold Medal in the year 2010. He has more than 14 years of teaching experience in handling subjects like Automata Languages and Computation, Information Security and Compiler Design. His fields of interest include Mobile Ad hoc Networks and Software Engineering.

G. Sandhya is currently working as Assistant Professor in the Department of Computer Science and Engineering at Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India. She received her Master's degree in the year 2013 from Anna University, Chennai, Tamilnadu, India. She has 3 years of teaching experience. Her research interests include Data Mining and IoT networks. She has published around 10 papers in Journals and Conferences. She is a member in IAENG.

G. Aishwaryalakshmi is currently working as Assistant Professor in the Department of Information Technology at Sri Krishna College of Technology, Coimbatore, Tamilnadu, India. She received her Master's degree in the year 2015 from Anna University, Chennai, Tamilnadu, India. Her research interests include Cloud and IoT networks.