Source Anonymization Using Modified New Variant ElGamal Signature Scheme

JHANSI VAZRAM. B[1], VALLI KUMARI. V[2], MURTHY J.V.R[3]
[1]Department of Computer Science and Engineering
Narasaraopeta Engineering. College
Narasaraopet - 522601
[2]Department of Computer Science and Systems Engineering
College of Engineering (A), Andhra University
Visakhapatnam - 530003
[3]Department of Computer Science and Engineering
College of Engineering (A), J N T University
Kakinada - 533003
INDIA
jhansi.bolla@gmail.com, vallikumari@gmail.com, mjonnalagedda@gmail.com

Abstract: - Mobile ad hoc networks (MANETs) have distinct features: like dynamic nodes, changing topologies, nodes cooperation and open communication media. Anonymity of message contents and participants is the most concerned task in MANET communication. Most of the existing methods face a challenge due to heavy cryptographic computation with high communication overheads. In this paper we propose an unconditionally secure privacy preserving message authentication scheme (PPMAS), which uses Modified New variant ElGamal signature Scheme (MNES). This scheme enables a sender to transmit messages, providing authentication along with anonymity, without relying on any trusted third parties. It also allows the untraceability of the link between the identifier of a node and its location. The experimental analysis of the proposed system is presented.

Key-Words: - Network security, Anonymity, Privacy, Mobile ad hoc networks, PPMAS, MNES.

1 Introduction

A set of mobile wireless devices having the capability of relaying packets for another in a cooperative manner is called as a mobile ad hoc network (MANET). The advantage of a MANET is that the disadvantages of wired networks and centralized administration issues are solved. The applications of MANET are manifold: battle ground communication, disaster recovery, conferencing and information sharing. The communication between the mobile nodes normally is performed through multi hop paths.

The main concern with the MANET is that the information about the nodes and their networks is to be made public. Many applications find this as a privacy threat. A node should be able to preserve its identity, its location and its network neighbours [8][17]. This privacy can be achieved using encryption.

The nodes in MANETs must be able to communicate messages in an authenticated manner securely. In addition to this the privacy of the node should be preserved making the node anonymous. Wireless MANETs are often found deployed where unfavorable conditions deter the deployment of a fixed wire network, where anonymity may be highly desirable for participating nodes. Consider a scenario in which members of an underground movement wish to share news about the crimes of an oppressive regime. Can an attacker detect who is producing the information and who is consuming it? Can an attacker ascertain other relationships between participating nodes and consequently punish them? Alternatively, consider a mobile combat unit operating inside enemy territory. Given that an enemy has set up a sensor network to eavesdrop on all communications, does the enemy know which node serves as a central leader or where forces are concentrated?

On account of quandaries such as these, anonymity in MANETs has become a subject of research in recent years, with several anonymization schemes proposed and analyzed. These include refurbished wired network schemes as well as specially tailored new ones. However, most existing schemes require use of heavy cryptography, pre-existing trust among nodes or dissemination of complete knowledge of network topology. These requirements are not aligned with typical MANET constraints, whereby nodes need to conserve energy, do not necessarily know each other in advance and may often move about, respectively. Moreover, adversaries encountered in wireless MANETs are quite different from those encountered in fixed networks, due to increased node vulnerability and the nature of the wireless medium. Hence, anonymity in MANETs requires rethinking. In this work, we examine it a new.

Outline of the paper: Section 2 presents the related work done. Section 3 gives an overview of the proposed privacy preserving unconditionally secure message authentication scheme (PPMAS). Section 4 discusses security analysis. Performance analysis is given in section 5. Finally, section 6 concludes the paper and suggests possible extensions.

2 Related Work

2.1 Terminology and preliminary

Unlinkability of an entity with a message or an action performed by it means that an adversary with enough information is unable to identify the identity of the entity, given the message or an action performed by it. Unlinkability makes anonymity possible. Privacy of both the source and the destination has to be protected in MANETs. It is also desirable that the attacker should not be able to derive the fact that source and destination nodes are communicating. We define a set of objects called anonymous set (AS) to see that a particular object is unidentifiable.

Our proposed work, like any other signature schemes consists of two algorithms, GEN and VER. With GEN algorithm, given the message m and the public keys of anonymous set (AS), a sender from AS, with her own private key, can generate an anonymous message $\mathcal{s}(m)$. The VER algorithm, given the message m and anonymous message $\mathcal{s}(m)$, is used to verify whether $\mathcal{s}(m)$ is generated by a member in the AS. The security requirements for our method are sender anonymity and Unforgeability.

AS or $\mathcal{s}$	Anonymity set
M	Message
$\mathcal{s}(m)$	PPMAC of the message
x_i	private key of the ith user
r_i	ith signature component 1
s_i	ith signature component 2
y_i	public key of the ith user for the PPMAC generation
N	number of users in $\mathcal{s}$
P	a large prime number
A	a primitive element in Z_p
Z_p	Integer field modulo p
H	hash function, like SHA-1
h_i	hash value, $h_i = H(m, r_i s_i)$
W	verification parameter
MNES	Modified new variant ElGamal signature scheme
PPMAC	Privacy preserving message authentication code
PPMAS	Privacy preserving message authentication scheme
KEY_GEN	Key generation algorithm
SIG_GEN	Signature generation Algorithm
VER	Verification algorithm

Table 1 Notations used

2.2 A discussion on existing works

The existing anonymous communication protocols are largely stemmed from either mixnet [2] or DC-net [4]. The secrecy of user's communication relationship can be protected by using mixnet. Anonymity can be provided by packet reshuffling through at least one trusted "mix". The outgoing message and the ID of the recipient are encrypted by the sender using the public key of the "mix". A batch of encrypted messages will be accumulated at the mix, it then decrypts and reorders those messages and forwards them to recipients. Therefore an eavesdropper is unable to link a decrypted output message with any particular encrypted input message. Recently, Moler presented a secure public-key encryption algorithm for mixnet [10]. This algorithm has been adopted by Mixminion [9]. However, since mixnet like protocols rely on the statistical properties of background traffic, they cannot provide provable anonymity.

Crowds [13] extends the idea of anonymizer and is designed for anonymous web browsing. However, Crowds only provides sender anonymity. Packet content and receivers would not be hidden by the en route nodes. Hordes [11] builds on the Crowds. It provides only sender anonymity and uses multicast services.

DC-net [4, 6] is an anonymous multiparty computation amongst a set of participants, some pairs of which share secret keys. Without the need of trusted servers DC-net provides perfect sender anonymity. In order to achieve receiver anonymity users have to send encrypted broadcasts to the entire group. However, DC-net gives different level of sender-receiver anonymity, because all group members get aware of when a message is sent. In addition, DC-net takes additional band width to handle collisions and contention, as only one user could send at a time. Finally, when a DC-net participant is joining the system, it fixes DC-net's tradeoff between anonymity and band width, but when others are joining there are no provisions to rescale.

Recently, message sender anonymity based on ring signatures was introduced [7] and [12]. This method provides an assurance to the sender that the generated message has source anonymous signature along with content authenticity, while hiding the message sender's real identity. The major idea is that the message sender (say Alice) randomly selects *n* of ring members as the AS on her own without awareness of these members.

To generate a ring signature, for each member in the ring other than the actual sender (Alice), Alice randomly selects an input and computes the one-way output using message signature forgery. To perform trapdoor one-way function, the actual sender Alice, using her knowledge of the trap-door information, tries to solve the "message" that can "glue" the ring together, and then signs this "message". The original scheme has very limited flexibility and the complexity of the scheme is quite high. Moreover, the Original paper only focuses on the cryptographic algorithm, the relevant network issues were totally left unaddressed.

In this paper, we propose an unconditionally secure privacy preserving message authentication scheme (PPMAS) based on the modified new variant ElGamal signature scheme. This is because the original ElGamal signature scheme is existentially forgeable with a generic message attack [14, 15]. While the modified ElGamal signature (MES) scheme [7] is secure against no-message attack and adaptive chosen message attack in the random oracle model [16], it cannot be used for more than one message. The modified new variant ElGamal signature scheme (MNES) is almost very similar to MES, and also [3] we can transmit more than one message without changing the secret exponents.

3 Our Work

In this section, we propose an efficient privacy preserving unconditionally secure message authentication scheme (PPMAS). The main idea is that for each message m to be released, the sending node generates a privacy preserving message authentication for the message m. The generation is based on the MNES scheme discussed in 3.1. Unlike ring signatures, which require computing a forgery signature for each member in the AS separately, our scheme only requires three steps to generate the entire PPMAS. This scheme links all non-senders and the message sender to the PPMAS alike. In addition, our design enables the PPMAS to be verified through a single equation without verifying the signatures individually.

3.1 Modified New variant ElGamal Signature scheme (MNES) Algorithm

The NES [3] is based on the difficulty of computing discrete logarithms and is based on schemes originally presented by ElGamal [1] and Schnorr [18]. Even though it relies on an ElGamal similar equation with three unknown variables, it has the following advantages.

- It avoids the extended Euclidean algorithm
- Sender can sign two messages with the same couple of secret exponents.

Based on the NES [3], we propose a modified new variant ElGamal signature (MNES) algorithm. To generate a signature and to verify it for a message m, using Modified New variant Signature scheme(MNES).

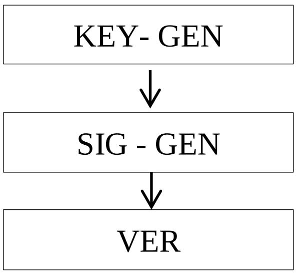

Fig.1. Algorithms used for MNES

Algorithms used for MNES are defined as follows:

1) KEY_GEN algorithm

- Global public key components
  p: a large prime
  α: generator of Z_p^*

- User’s private key
  x:a random number, $x \in Z_p^*$

- User’s public key
  y:$y = \alpha^x \, mod \, p$

- User’s secret exponents
  k, l: random numbers, $k, l \in Z_{p-1}^*$

2) SIG_GEN algorithm

$$r = \alpha^k \, mod \, p$$
$$s = \alpha^l \, mod \, p$$
$$q = \alpha^h \, mod \, p \quad \text{where h=h(m, rs)}$$
$$w = k + l + q + xr + ks + lq \, mod \, (p-1).$$

Signature = (r, s, w).
where r, s are signature components, k and l are secret exponents and w is a verification parameter.

3) VER algorithm

The verifier checks the signature equation

$$\alpha^w = rsqy^r r^s s^q \, mod \, p.(1)$$

If the equality (1) holds true, then the verifier accepts the signature and rejects otherwise.

The generation and verification of MNES is diagrammatically represented in Fig.1.

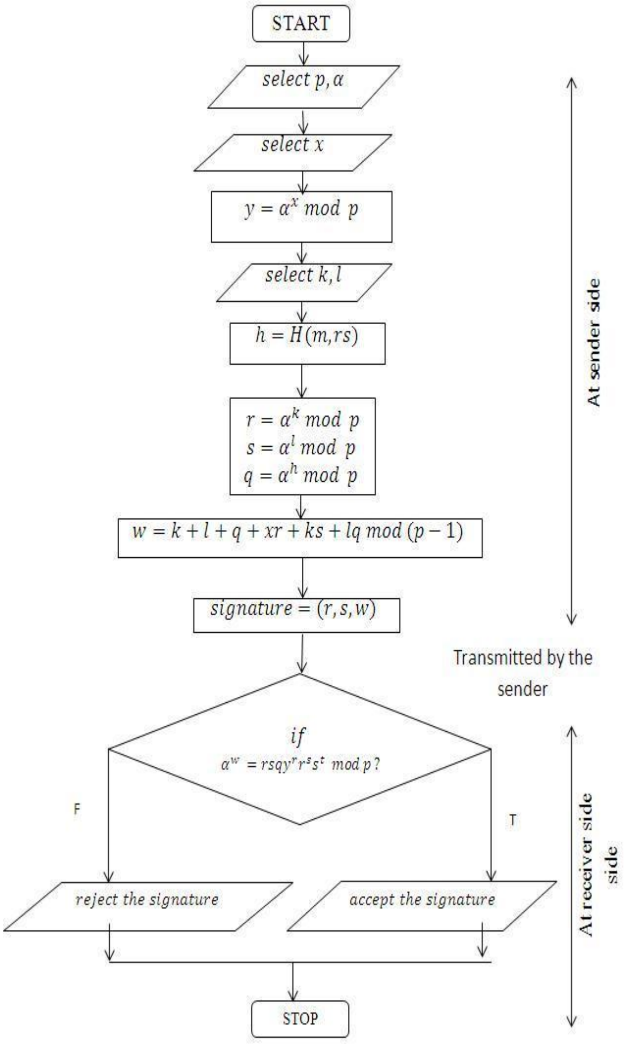

Fig.1. Generation of MNES scheme

3.2 Unconditionally secure PPMAS

Suppose that the message sender (say Alice) wishes to transmit a message m anonymously from her network node to any other node. The AS includes *n* members, $A_1, A_2, \ldots, A_n$, for example, $\mathcal{S} = \{A_1, A_2, \ldots, A_n\}$, where the actual message sender Alice is A_t, for some value t, $1 \le t \le n$.

Let *p* be a large prime number and α be a primitive element of Z_p^*. Then α is also a generator of Z_p^*.That is $Z_p^* = <\alpha>$. Both *p* and α are made public and shared by all members in $\mathcal{S}$. Each $A_i \in \mathcal{S}$ has a public key $y_i = \alpha^{x_i} mod \, p$, where x_i is a randomly selected private key from Z_{p-1}^*. In this paper, we will not distinguish between the code A_i and its public key y_i. Therefore, we also have $\mathcal{S} = \{y_1, y_2, \ldots, y_n\}$.

Suppose *m* is a message to be transmitted. The private key of the message sender Alice is x_t, $1 \le t \le n$. To generate an efficient PPMAC for message *m*, Alice performs the following two algorithms:

1. *SIG_GEN algorithm for PPMAS:*

- Compute $r_i = \alpha^{k_i} \, mod \, p$, $s_i = \alpha^{l_i} \, mod \, p$, $q_i = \alpha^{h_i} \, mod \, p$ for each $1 \le i \le n$, $i \ne t$, where k_i, l_i are random and pair wise different numbers in Z_p^* , and $h_i = H(m, r_i s_i)$. h is a hash function like SHA-1.

- Compute $r_t = \alpha^k \prod_{i \ne t} y_i^{-r_i} \, mod \, p$, $s_t = \alpha^l \prod_{i \ne t} r_i^{-s_i} \, mod \, p$, $q_t = \alpha^h \prod_{i \ne t} s_i^{-q_i} \, mod \, p$ for a random k, l

$\in Z_p^*$, h = H(m, rs), such that $r_t \neq 1$, $s_t \neq 1$, $h_t \neq 1, r_i \neq r_t$, $s_i \neq s_t, h_i \neq h_t$ for each $i \neq t$.

- Compute

$$w = k + l + h + \sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i + x_t r_t + k_t s_t + l_t q_t \ mod\ (p-1)$$

Then the signature is

$$\mathscr{s}(m) = (m, \mathscr{s}, r_1 \dots . r_n, s_1 \dots . s_n, q_1 . \dots q_n, w)$$

Where

$$\alpha^w = (r_1 \dots r_n s_1 \dots s_n q_1 \dots q_n y_1^{r_1} \dots y_n^{r_n} r_1^{s_1} \dots r_n^{s_n} s_1^{q_1} \dots s_n^{q_n})\ mod\ p$$

2. ***VER algorithm :***

The verifier verifies

$$\alpha^w = r_1 \dots r_n s_1 \dots s_n q_1 \dots q_n y_1^{r_1} \dots y_n^{r_n} r_1^{s_1} \dots r_n^{s_n} s_1^{q_1} \dots s_n^{q_n}\ mod\ p. \quad (2)$$

If (2) holds true, the verifier accepts the PPMAS as valid for message m. Otherwise the verifier rejects the PPMAS.

If the PPMAS has been correctly generated, then we have

$$\prod_{i=1}^n r_i \prod_{i=1}^n s_i \prod_{i=1}^n q_i \prod_{i=1}^n y_i^{r_i} \prod_{i=1}^n r_i^{s_i} \prod_{i=1}^n s_i^{q_i}\ mod\ p$$

$$= (\prod_{i\neq t}^n r_i)\, r_t (\prod_{i\neq t}^n s_i)\, s_t\, (\prod_{i\neq t}^n q_i) q_t (\prod_{i\neq t}^n y_i^{r_i})\, y_t^{r_t} (\prod_{i\neq t}^n r_i^{s_i})\, r_t^{s_t} (\prod_{i\neq t}^n s_i^{q_i}) s_t^{q_t}\ mod\ p$$

$$= \alpha^{\sum_{i\neq t} k_i} \alpha^{\sum_{i\neq t} l_i} \alpha^{\sum_{i\neq t} h_i} (\alpha^k \prod_{i\neq t} y_i^{-r_i}) (\prod_{i\neq t} y_i^{r_i})\, y_t^{r_t} (\alpha^l \prod_{i\neq t} r_i^{-s_i}) (\prod_{i\neq t} r_i^{s_i})\, r_t^{s_t}\ (\alpha^h \prod_{i\neq t} s_i^{-q_i}) (\prod_{i\neq t} s_i^{q_i})\, s_t^{q_t}\ mod\ p$$

$$= \alpha^{\sum_{i\neq t} k_i} \alpha^{\sum_{i\neq t} l_i} \alpha^{\sum_{i\neq t} h_i}\, \alpha^k\ y_t^{r_t}\, \alpha^l\, r_t^{s_t}\, \alpha^h\, s_t^{q_t}\ mod\ p$$

$$= \alpha^{\sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i + k + l + h}\, y_t^{r_t}\, r_t^{s_t}\, s_t^{q_t}\ mod\ p$$

$$= \alpha^{\sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i + k + l + h}\, \alpha^{x_t r_t} \alpha^{k_t s_t}\, \alpha^{l_t q_t}\ mod\ p$$

$$= \alpha^{k+l+h+\sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i + x_t r_t + k_t s_t + l_t q_t}\ mod\ p$$

$$= \alpha^w\ mod\ p.$$

Therefore PPMAS should always be accepted if it is correctly generated without being modified. As a trade-off between computation and communication, the PPMAS can also be defined as

$\mathscr{s}(m) = (m, \mathscr{s}, r_1 \dots . r_n, s_1 \dots . s_n, w)$. If $\mathscr{s}$ is also clear, it can be eliminated from the PPMAS.

The generation and verification of PPMAS(Privacy preserving message authentication scheme) is diagrammatically represented in Fig.2.

3.3 Node mobility

As far as the group is formed and maintaining without any disturbances, everything is well and good. Because of the dynamic nature [22] of the MANET nodes, a node may join or leave the group whenever it is willing to. This will be handled by a specially designated node in the group called special node.

3.3.1 New node joining the group

Whenever a new node, say A, wants to join in the group, it sends a request to special node. Depending on the signal strength received, the special node fixes the position of new node in the group. This information is broad casted to all other nodes in the group by the special node.

3.3.2 Existing node leaving the group

Whenever an existing node in the group say A, wants to leave the group, it sends leaving message to its neighbours as well as the special node. The special node broadcasts this information also to the group members.

Therefore, whenever a node wants to generate an anonymous message $\mathscr{s}(m)$, it considers received broadcast messages from the special node, regarding new node joining and existing node leaving. To generate an anonymous message, it requires public keys of all existing nodes in the ring. This information is required by the sending node to collect the public keys of the group members, which are required to generate $\mathscr{s}(m)$. But, the topology changes regarding the dynamic nature of MANET nodes will not affect the anonymous message generation by a node in the group.

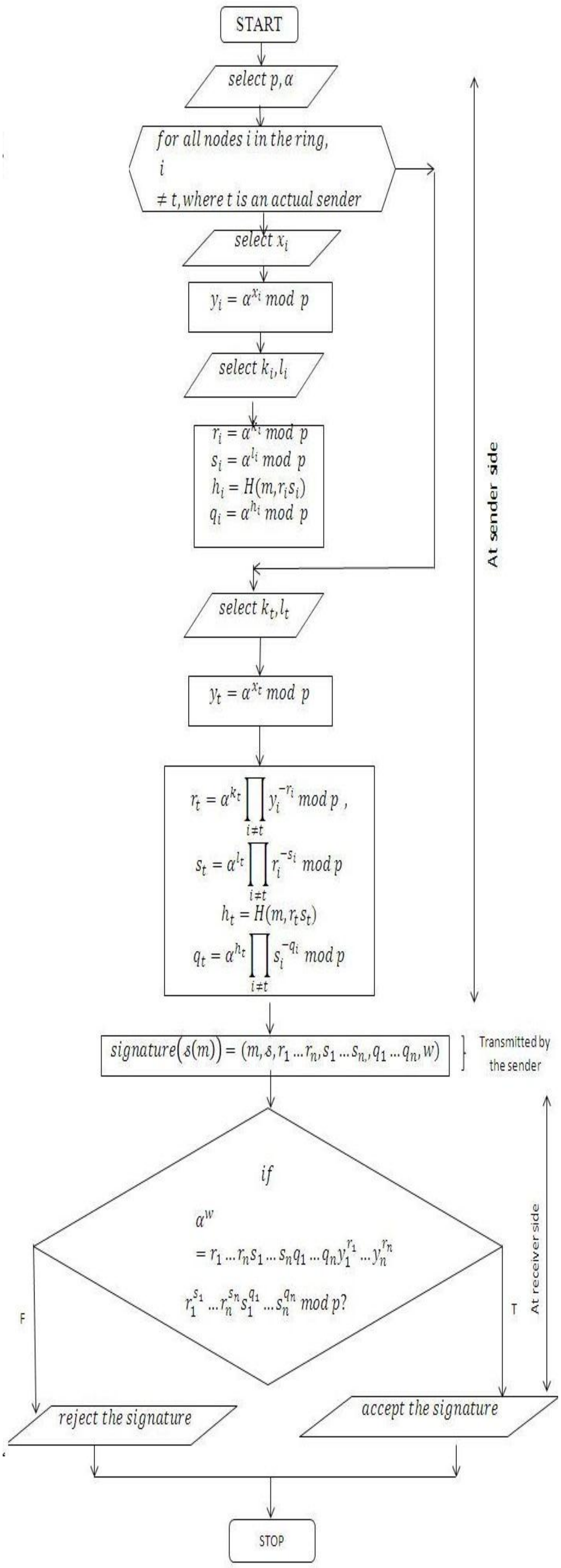
START
select p, α
for all nodes i in the ring, $i \neq t$, where t is an actual sender
select x_i
$y_i = \alpha^{x_i} \bmod p$
select k_i, l_i
$r_i = \alpha^{k_i} \bmod p$
$s_i = \alpha^{l_i} \bmod p$
$h_i = H(m, r_i s_i)$
$q_i = \alpha^{h_i} \bmod p$
select k_t, l_t
$y_t = \alpha^{x_t} \bmod p$
$r_t = \alpha^{k_t} \prod_{i \neq t} y_i^{-r_i} \bmod p$,
$s_t = \alpha^{l_t} \prod_{i \neq t} r_i^{-s_i} \bmod p$
$h_t = H(m, r_t s_t)$
$q_t = \alpha^{h_t} \prod_{i \neq t} s_i^{-q_i} \bmod p$
At sender side
$signature(\delta(m)) = (m, \delta, r_1 \ldots r_n, s_1 \ldots s_n, q_1 \ldots q_n, w)$
Transmitted by the sender
if
α^w
$= r_1 \ldots r_n s_1 \ldots s_n q_1 \ldots q_n y_1^{r_1} \ldots y_n^{r_n}$
$r_1^{s_1} \ldots r_n^{s_n} s_1^{q_1} \ldots s_n^{q_n} \bmod p?$
F
T
At receiver side
reject the signature
accept the signature
STOP

Fig.2. Generation of PPMAS

3.4 Integration with Mobile Ad Hoc Routing Protocols

3.4.1 Architecture of the network topology of our Work

Our proposed PPMAS may use the topology shown in Fig.3. Prior to the network deployment, the network administrator categorizes the ring nodes into ordinary nodes and special nodes, as indicated in the fig.2. Inter MANET node communication is possible through special nodes. Statically or dynamically generated pseudonyms can be assigned are assigned to special nodes to provide anonymous transmissions as in [7], [24], [26].

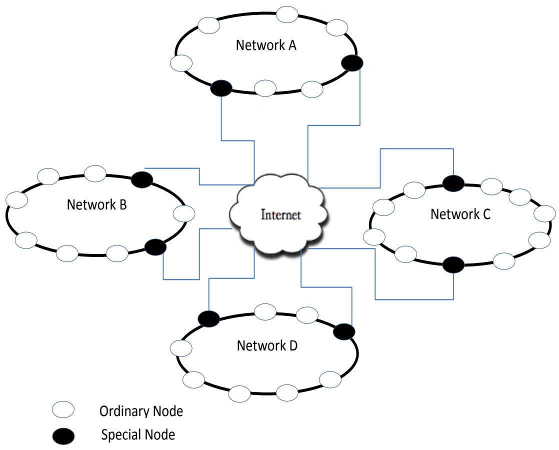

Fig.3. Network Topology Architecture

The proposed PPMAS can be integrated with all kinds of routing protocols, such as AODV [19], DSR [20], DSDV [21] and so on, of many types of wireless network, e.g. mobile ad hoc networks and wireless sensor networks.

4. Security analysis

In this subsection, we prove that the proposed PPMAS is unconditionally anonymous and provably unforgeable against adaptive chosen message attack: an adversary who receives signatures for messages of his choice cannot later forge the signature of even a single additional message.

4.1 Anonymity

To prove that the proposed PPMAS is unconditionally anonymous, we have to prove that

- For anybody other than the members of $\mathscr{S}$ the probability to successfully identify the real sender is 1/n.
- Anybody from $\mathscr{S}$ can generate PPMAS.

Axiom1. The proposed privacy preserving message authentication scheme (PPMAS) can provide unconditional message sender anonymity.

Proof. The identity of the message sender is unconditionally protected with the proposed PPMAS scheme. This is because that regardless of the sender's identity, there are exactly $(p - 1)(p - 2) \cdot\cdot\cdot (p - n)$ different options to generate the PPMAS, and all of them can be chosen by the PPMAS generation procedure and by any of the members in the AS with equal probability without depending on any complexity theoretic assumptions. The proof for the second part, that anybody from S can generate the PPMAS is straightforward.

4.2 Unforgeability

The design of the proposed PPMAS relies on the ElGamal signature scheme. Different levels of security can be achieved by signature schemes. The maximum level of security is a counter to existential forgery under adaptive chosen message attack. In order to discuss counter measure to chosen message attack for PPMAS, we proved the following theorem. In this connection we define first a verification parameter.

Definition: Let $r_i = \alpha^{k_i}\ mod\ p$, $s_i = \alpha^{l_i}\ mod\ p$, $q_i = \alpha^{h_i}\ mod\ p$, $r_t = \alpha^k \prod_{i\neq t} y_i^{-r_i}\ mod\ p$, $s_t = \alpha^l \prod_{i\neq t} r_i^{-s_i}\ mod\ p$, $q_t = \alpha^h \prod_{i\neq t} s_i^{-q_i}\ mod\ p$. We define verification parameter w such that $w = k + l + h + \sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i + x_t r_t + k_t s_t + l_t q_t\ mod\ (p - 1)$.

Axiom 2. A sender can sign two messages with same pair of secret exponents.

Proof. Consider a MANET with n nodes $A_1, A_{2,} \ldots . A_n$. Let a node A_t, where $1 \leq t \leq n$ be the actual sender. Let m_1 and m_2 be two different messages with different verification parameters w_1 and w_2 respectively. For these two different messages, we assume that they have same couple of secret exponents k_i and l_i where $1 \leq i \leq n$. We know that $r_i = \alpha^{k_i}\ mod\ p,\ s_i = \alpha^{l_i}\ mod\ p$ which follows that $r_i's, s_i's$ are same for the two messages m_1 and m_2. Now we can take the signatures of two messages m_1 and m_2 as $(r_1 \ldots . r_n, s_1 \ldots . s_n, w_1)$ and $(r_1 \ldots . r_n, s_1 \ldots . s_n, w_2)$ respectively. By the definition of verification parameter, we have

$$w_1 \equiv k_t + l_t + h_t + \sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i + x_t r_t + k_t s_t + l_t q_t\ mod\ (p-1)$$

$$w_2 \equiv k_t + l_t + h_t' + \sum_{i\neq t} k_i + \sum_{i\neq t} l_i + \sum_{i\neq t} h_i' + x_t r_t + k_t s_t + l_t q_t'\ \ mod\ (p-1)$$

For some large prime p and x_t is the private key of A_t. Where $h_t = h(m_1, r_t s_t)$, $q_t = \alpha^{h_t}\ mod\ p$, $h_t' = h(m_2, r_t s_t)$, $q_t' = \alpha^{h_t'}\ mod\ p$, h is a hash function like SHA-1.

Then, $w_1 - w_2 \equiv h_t - h_t' + \sum_{i\neq t}(h_t - h_t') + l_t(q_t - q_t')\ mod\ (p-1)$

$$w_1 - w_2 \equiv l_t(q_t - q_t')\ mod\ (p-1)$$

$$w_1 - w_2 = l_t(q_t - q_t') + L\ (p-1)$$

Let $gcd(q_t - q_t',\ p - 1) = d$

$$q_t - q_t' = dQ$$

$p - 1 = dP$ Where $P, Q\ \in Z_p^*$; $\gcd(P, Q) = 1$

$$w_1 - w_2 = l_t dQ + LdP\ \ mod\ P$$

$$w_1 - w_2 = d(l_t Q + LP)\ mod\ P$$

$w_1 - w_2 = dM\ mod\ P$ where $M = l_t Q + LP$

$$\Rightarrow M = l_t Q\ mod\ P$$

$$\Rightarrow l_t = MQ^{-1}\ mod\ P$$

$[\because \gcd(P, Q) = 1, Q\ is\ invertible\ with\ respect\ to\ P]$

$\Rightarrow l_t = MQ^{-1} + L'P$ where $L' \in Z_p^*$.

Without the loss of generality, we can assume that $L' = L$.

$\Rightarrow l_t = MQ^{-1} + LP$ (3)

Now $l_t < p-1$ as we know that $s_t = \alpha^{l_t} \prod_{i \neq t} r_i^{-s_i} \ mod\ p$

$$\Rightarrow l_t < p$$

$$\Rightarrow l_t < dP + 1$$

$$\Rightarrow l_t \leq dP$$

$\Rightarrow MQ^{-1} + LP \leq dP$

$$\Rightarrow MQ^{-1} \leq P(d - L)$$

This is possible if $d - L > 0, \Rightarrow L < d$

Now by (3), we can test every value of L and check with $s_t = \alpha^{l} \prod_{i \neq t} r_i^{-s_i} \ mod\ p$. Even though we can find l_t, it is very difficult to find out $k_t\ and\ x_t$, which leads the theorem.

4.2.1 PPMAS is unforgeable

In connection with the above theorem, one may infer that, the proposed PPMAS is unforgeable. With two different messages m$_1$ and m$_2$ having different verification parameters w_1 and w_2, same k_t, l_t (secret exponents) and x_t (private key), an attacker can identify one of the secret exponents l_t. But it is computationally infeasible for him to deduce k_t and x_t using the known l_t. Therefore our proposed PPMAS is secure enough against existential forgery attack. Hence PPMAS is unforgeable.

4.3 Integration with privacy preserving communication protocols

PPMAS is used to provide only sender anonymity, when a sending node is in a group i.e., in a ring topology or in a coalition. To achieve full anonymity using PPMAS, one has to transmit the source anonymous message using a privacy preserving communication protocol like the one in [7].

5 Performance Analysis

The execution of PPMAS system grows with an increase in the number of nodes in the $O(n^2)$, where n is the number of nodes. If we take number of nodes in the group on x- axis and time in seconds on y-axis, the resultant graph which shows the performance of PPMAS is as shown in Fig.1. It is clearly observable that when the number of nodes increases consistently, the time take for the nodes to generate PPMAS will increase accordingly.

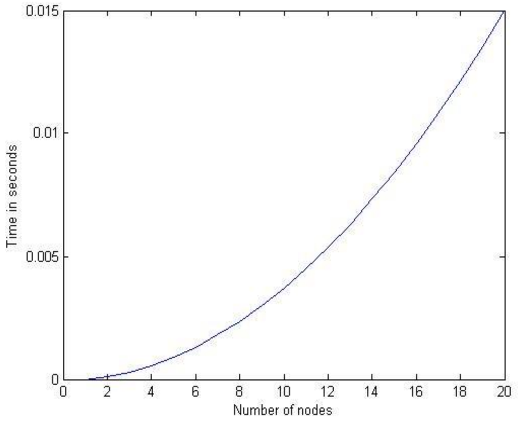

Fig. 4. Performance analysis of PPMAS

5 Conclusions

The paper has proposed an unconditionally secure privacy preserving message authentication scheme using another newly proposed modified new variant ElGamal signature scheme. The anonymity and Unforgeability properties of this scheme were proved. A critical security analysis of said scheme was performed. It was observed that the link between identifier of a node and its location is hidden. Another advantages of this scheme is that the trusted third parties are not required and more than one message is signed with the same signature.

This scheme can be used with any wireless adhoc networks with ring topology. This paper proposes a method to anonymize source, but when implemented with appropriate routing protocol, full anonymity (source anonymity, relationship anonymity and destination anonymity) can be achieved.

References:

[1] ElGamal, T., A Public-key Cryptosystem and a Signature Scheme based on Discrete Logarithms, IEEE Transactions on Information Theory, July 1985

[2] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, vol. 24, 1981, pp.84 – 88.

[3] Omkar Khadir, New Variant of ElGamal Signature Scheme, *Int. J.Contemp.Math.Sciences*, Vol. 5, 2010, no.34, pp. 1653-1662.

[4] D. Chaum., The dining cryptographers problem: unconditional sender and recipient untraceability, *Journal of Cryptology*, vol. 1, no. 1, 1988.3es, pp. 65–75.

[5] M. Reed, P. Syverson, and D. Goldschlag. Anonymous connections and onion routing, *IEEE journal on Selected Areas in Communications*, vol. 16, no. 4, 1998, pp. 482–494.

[6] M.Waidner, Unconditional sender and recipient untraceability in spElGaite of active attacks, P*roc. of the Workshop on the Theory and Application of Cryptographic Techniques (Eurocrypt '89)*, vol. 434 of Lecture Notes in Computer Science, Houthalen, Belgium, Apr. 1989, pp. 302–319.

[7] Ian Ren, Yun Li, and Tongtong Li, SPM: Source Privacy for Mobile Ad Hock Networks, in *EURASIP Journal on wireless communications and networking*, vol.2010, article ID534712, 10 pages.

[8] M.G. Reed, P. F. Syverson, and D. M. Goldschlag, Anonymous Connections and Onion Routing, *Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection*, 1998.

[9] G.Danezis, R. Dingledine, and N. Mathewson, Mixminion: design of a type III anonymous remailer protocol, *Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, Calif, USA, May2003, pp. 2–15.

[10] B. Moller, Provably secure public-key encryption for length preserving chaumian mixes, *Proc. of the Cryptographer's Track at the RSA Conference (CT-RSA '03)*, vol. 2612 of Lecture Notes in Computer Science, San Francisco, Calif, USA, Apr. 2003, pp.244–262.

[11] C. Shields and B. N. Levine. "A protocol for anonymous communication over the Internet." in *Proc. of the 7th ACM Conference on Computer and Communication Security*, D. Gritzalis, Ed., ACM Press, Athens, Greece, Nov. 2000.

[12] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret, *Proc. of the 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '01)*, vol. 2248 of Lecture Notes in Computer Science, Springer, Gold Coast, Australia, Dec. 2001.

[13] M. Reiter and A. Rubin, Crowds: anonymity for web transaction, *ACM Transactions on Information and System Security*, vol. 1, no. 1, 1998, pp. 66–92.

[14] T. A. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol. 31, no. 4, 1985, pp. 469–472.

[15] S. Goldwasser, S. Micali, and R. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, *SIAM Journal on Computing*, vol. 17, 1988, pp. 281–308.

[16] D. Pointcheval and J. Stern, Security proofs for signature schemes, *Proc. of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '96)*, vol. 1070 of Lecture Notes in Computer Science, Saragossa, Spain, May 1996, pp. 387–398.

[17] M.K. Reiter and A. D. Rubin. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, *Symposium on Security & Privacy*, Oakland, Calif, USA, May 2003.

[18] Schnorr, C., Efficient Signatures for Smart Card, *Journal of Cryptography*, vol. 3, 1991.
C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector (aodv) routing," Internet Draft, Feb 2003, http://www.ietf.org/internetdrafts/draft-ietf-manet-aodv-13.txt.

[19] D. B. Johnson, D. A. Maltz, and Y.-C. Hu,"The dynamic source routing protocol for mobile adhoc networks (dsr)," Internet Draft, Apr 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.

[20] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," in *Proceedings of the ACM Conference on Communications Architectures, Protocols And applications (SIGCOMM'94) London, UK:ACM Press, 1994.*

[21] A.Subramani and A. Krishnan, Node Mobility Tracking In Mobile Ad-Hoc Networks in their geographical position (Dynamic Networks),

International Journal of Soft Computing and Engineering(IJSCE), ISSN:2231-2307,Vol.1,Issue-5,September 2011.

[22] Yanchao Zhang, Wei Liu and Wenjing Lou, Anonymous Communications in Mobile Ad Hoc Networks, 2005 IEEE.

[23] Carlos T. Calafate, Javier Campos, Marga N´acher, Pietro Manzoni, and Juan-Carlos Cano, A-HIP: A Solution Offering Secure and Anonymous Communications in MANETs, IWSEC 2010, LNCS 6434, 2010, Springer-Verlag Berlin Heidelberg 2010, pp.217–231.

[24] Huseyin Can, Anonymous Communications in Mobile Ad Hoc Networks, Kongens Lyngby 2006 IMM-M.Sc-2006-91.

[25] ElGamal T.A., A public-key cryptosystem and a signature scheme based on discrete Logarithms. IEEE Transactions on Information Theory, vol. 31, no. 4, 1985, pp. 469–472.

[26] Stallings W., *Cryptography and Network Security*, Pearson Education, 4-th Edition. 2010.

[27] Zhang R., Zhang Y., Fang Y., AOS: An anonymous overlay system for mobile ad hoc networks , Springer Science+Business Media, 2011.

[28] Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B., Shields, C., & Belding-Royer, E. Authenticated routing for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 2005, pp. 598-610.

[29] Danezis, G., Diaz, C., Kasper, E., Torncoso, C. The wisdom of Crowds: Attacks and optimal constructions. In ESO-RICS’09 St Malo, Framce, 2009

[30] Javier C., Calos Calafate, T., Nacher, M., Manzoni, P., Carlos Cano, J. Hop: Achieving Efficient Anonymity in MANETS by Combining HIP, OLSR and Pseudonyms. *EURASIP Journal on Wireless Communications and Networking,* 2011.