View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Research Online

University of Wollongong

Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

16-11-2005

Secure and anonymous mobile ad-hoc networks

Y. Mu
University of Wollongong, ymu@uow.edu.au

F. Zhang
Sun Yat-Sen University, fzhang@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/infopapers

Part of the Physical Sciences and Mathematics Commons

Recommended Citation

Mu, Y.; Zhang, F.; and Susilo, Willy: Secure and anonymous mobile ad-hoc networks 2005.
https://ro.uow.edu.au/infopapers/463

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Secure and anonymous mobile ad-hoc networks

Abstract

A mobile ad-hoc network (MANET) is a wireless network made up of mobile hosts that do not require any fixed infrastructure to communicate. The major features of ad-hoc networks is self-organization and dynamics in user participation. Because of these features, the security in ad-hoc becomes a challenge. In this paper, we consider an interesting scenario, where an arbitrary number of nodes in MANET can dynamically form an anonymous group that exhibits the following features: (1) any outsider can be convinced that the node is indeed in the group; (2) any outsider can send a message back to the node in the group.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as: Mu, Y, Zhang, F & Susilo, W, Secure and anonymous mobile ad-hoc networks, 2005 IEEE 7th Malaysia International Conference on Communication and the 13th IEEE International Conference on Networks, 2005, 16-18 November 2005, 2. Copyright IEEE 2005.

This conference paper is available at Research Online: https://ro.uow.edu.au/infopapers/463

Secure and Anonymous Mobile Ad-Hoc Networks

Yi Mu, Fangguo Zhang, and Willy Susilo

Abstract— **A mobile ad-hoc network (MANET) is a wireless network made up of mobile hosts that do not require any fixed infrastructure to communicate. The major features of ad-hoc networks is self-organization and dynamics in user participation. Because of these features, the security in ad-hoc becomes a challenge. In this paper, we consider an interesting scenario, where an arbitrary number of nodes in MANET can dynamically form an anonymous group that exhibits the following features: (1) any outsider can be convinced that the node is indeed in the group; (2) any outsider can send a message back to the node in the group.**

Keywords: Ad-hoc network, Security, Authentication, Confidentiality

I. Introduction

Security services in the MANET context faces many challenges. The insecurity of the wireless links and relatively poor physical protection of nodes in a hostile environment are major challenges. Nevertheless, the most important feature in MANET is the absence of a fixed infrastructure. The absence of infrastructure and the consequent absence of authorization facilities is the major hurdle in security, separating nodes into trusted and non-trusted. Since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Additionally, in MANET freely roaming nodes form transient associations with their neighbors, join and leave MANET independently and without notice. It may be difficult in most cases to have a clear picture of the ad hoc network membership. Consequently, no form of established trust relationships among the mobile nodes could be assumed.

In this paper, we consider a privacy issue where some mobile nodes in a MANET want to be anonymous during communication. It works as follows. Let Alice and Bob be two nodes in an n node MANET. Both want to hide their identity but each knows the receiver belongs to a group of nodes. Each party proves that she/he is indeed in the group to the other party without revealing his/her identification. They can also collaboratively establish an anonymous and secure communication channel during the process of the proofs; namely, they find a common communication cryptographic key. Their communication is then implemented by broadcast. Although all nodes can receive the broadcasted message, only Alice and Bob can find the plaintext message.

We achieve our system by utilizing the notion of ring signature along with traceability. The notion of ring signature was introduced by Shamir *et al.*[1]. A ring signature scheme allows a signer in a ring to construct a signature such that the receiver of the signature is assured that the signer is indeed a user in the ring, while the identification of the signer is indistinguishable to him. It poses a problem when the signer wants to receive an acknowledgment from the receiver and can claim that he has indeed received it without revealing his identification.

One of well-known ring signature constructions is the Abe-Ohkubo-Suzuki ring signature scheme [2]. They gave a generic scheme and provided three concrete schemes based on the Schnorr signature scheme, the RSA signature scheme, and a mix of both. The Abe-Ohkubo-Suzuki ring signature scheme provides full signer-indistinguishability with a perfectly closed ring. Taking a closer look at the scheme, we find that the signer-indistinguishability in the scheme stems from the fact: a resulting ring signature implies polynomially-m signers ($1 \leq m \leq n$). In other words, a ring signature can be imagined having constructed by m users in the ring. This might sometimes be problematic when the receiver wants to ensure the certainty of the number of users involved in the specific signature.

Our Contribution. We apply the notion of ring signature to MANET and show how to send a message to an anonymous user in a MANET. The contribution in this paper is twofold. (1) We propose a ring signature scheme that ensures certainty to the number of signers in a ring signature. (2) With this scheme, we are able to find a method of sending a message back to the ring. Let $\mathcal{U}$ be a group of n users in the ring. Let σ be a ring signature constructed by 1 out of n users in the ring. Upon receiving σ, the receiver is assured that σ is indeed constructed by a node in the MANET. The receiver can then send a message back to the signers without revealing the identifications of the signing node.

It is important to note that our solution is *different* from the trivial solution; namely, the signer embeds a random public key in the ring signature and then the receiver of the ring signature encrypts a message with the public key. Our argument to the trivial solution is that since the Abe-Ohkubo-Suzuki ring signature implies polynomial-m ($m > 0$) signers for a signature, the message sender is not sure who is/are the receiver(s) (or original signer(s)). In our scheme, the signer actually proves his knowledge of his respective private key wrt his public key; therefore, the originality of the single receiver of the encrypted message is guaranteed.

The rest of this paper is organized as follows. Section 2 reviews some previous works which are closely related to our scheme. Section 3 provides the definitions of our system including the security requirements. Section 4 presents a concrete scheme of 1-of-out-n ring signatures. Our scheme is based on the Abe-Ohkubo-Suzuki ring signature scheme

Yi Mu is with the School of IT and Computer Science, University Wollongong, Australia

Fangguo Zhang is with Department of Electronics and Communication Engineering, Sun Yat-Sen University, P. R. China

Willy Susilo is with the School of IT and Computer Science, University Wollongong, Australia

1-4244-0000-7/05/$20.00 ©2005 IEEE.

[2]. We provide a security proof to our scheme. We prove that our scheme is secure existentially unforgeable against adaptive chosen message attacks. The final section concludes this paper.

II. Related Work

Signer anonymity in digital signature is a cryptographic primitive, which has been extensively studied. There have been a number of schemes associated with signer anonymity in the literature, for instance, group signature and ring signature.

The concept of group signatures was initially introduced by Chaum [3]. In a group signature scheme, the signers are confined in a group managed by a group manager and a revocation manager. Any signer in the group can sign on the group behalf, but its identity remains secret to others including the group manager. The revocation manager can retrieve its identity when something goes wrong. The Chaum's signature scheme does not possess some desirable properties, for example, signer identities are known to the group manager, group signatures are traceable, and computational complexity is proportional to the size of a group. Since then, several major improvements have been proposed (e.g., [4], [5], [6], [7], [8]), in terms of computational efficiency, signer privacy, and security.

In 2001, Shamir *et al.* introduced a new notion: ring signature [1]. Unlike group signatures, a ring signature scheme provides unconditional signer anonymity; that is, signer's identities are hidden against all other parties, because there are no group manager and revocation manager in the ring (or group). There have been a number of ring signature constructions which are published, for example, Abe-Ohkubo-Suzuki's one of out n signature schemes [2], Zhang-Kim's ID-based ring signature scheme from pairings [9]. The former scheme is based on a closed hash chain. Any user in the chain can be the potential signer of a ring signature. Their system allows users to have a different cryptographic setup, so they do not have to be set up for a ring signature. They can be any users selected from a unknown entity. The later scheme is based on the Abe-Ohkubo-Suzuki's scheme, however, they allow the signer to include all identities in a ring signature using the technology of bilinear pairings.

User anonymity can also be achieved using the technique of mix-net. Mix-net is a cryptographic system introduced by Chaum [10] for providing communication unlinkability and anonymity. Mix-net are among the most widely used cryptographic tools for providing communication privacy. A mix-net consists of a number of mix-centers which permute the list of inputs (ciphertext) from the senders by re-encrypting the messages such that the output list from a mix-net has a different order of the input. Therefore, the receiver cannot learn who is the original message sender.

We recall the notions that are related to our work as follows. We concern both sender privacy *and* receiver privacy. We extend the Abe-Ohkubo-Suzuki ring signature scheme [2] to provide certainty to the number of signers in a ring. We allow a sender to send a message or messages to a ring such that the identification(s) of the receiver(s) is not revealed. It is noted that the Abe-Ohkubo-Suzuki ring signature scheme has be extended to the linkable ring signatures [11], where a signatures from a signer can be linked. Our notion differs from it, since we do not require linkability in our scheme. It is also noted that a threshold ring signature scheme has been proposed [12]. They allow m out of n users in a ring to construct a ring signature. We must stress that our scheme not only achieves this property, but also allows the signers to be fixed and the receiver to send messages back to the signers.

III. Definitions

In this section, we describe the formal definitions of our scheme and give the security definition to our scheme. We assume that all nodes have obtained a public key certificate from a trust certification agent prior to joining the MANET. All nodes periodically broadcast their certificates to the network.

Definition 1: 1-out-of-n signature $\mathcal{R}_n^1$ is a ring signature scheme comprised of the following algorithms:

- $\mathcal{R}$-*Setup*: is a probabilistic algorithm that on input a security parameter ℓ, outputs definitions of the set of users $\mathcal{U}$, the message space $\mathcal{M}$, the ring signature space $\mathcal{S}_r$, the public keys $L = \{y_i\}$ of all users in the ring. Each user in the ring obtains the associated private key x_i corresponding to y_i. All other parameters are denoted by π.
- RSign_n^1 is a probabilistic algorithm used by 1 out of n nodes in $\mathcal{U}$. It takes as input $\langle \{x_i\}_{i\in\mathcal{S}_m}, L, M_r \rangle$, where $\mathcal{S}_m$ denotes a subgroup of m nodes, $\{x_i\}_{i\in\mathcal{S}_m}$ are the private keys corresponding to $\{y_i\}_{i\in\mathcal{S}_m}$, L denotes all public keys in the ring, and $M_r \in \mathcal{M}$, outputs a ring signature $\sigma = \langle c_0, s_0, \cdots, s_{n-1}, \{A_j\}_{j\in\mathcal{S}_m}, M_r \rangle$ and a proof of the equality of discrete logs on x_j from $\{y_i\}_{i=0,\cdots,n-1}$ and $\{A_j\}_{j\in\mathcal{S}_m}$., where $\{s_i\} \in \mathcal{S}_r$, c_0 is the associated parameter, each element in $\{A_j\}_{i\in\mathcal{S}_m}$ is a function of one element in $\{x_i\}_{i\in\mathcal{S}_m}$.
- $\mathsf{RVerify}_n^1$ is a deterministic algorithm that takes as input $\langle \sigma, L \rangle$, and outputs accept or reject.

The security of the $\mathcal{R}_n^1$ signature scheme has two aspects: $\mathcal{R}_n^1$ signer ambiguity and unforgeability. The $\mathcal{R}_n^1$ signer ambiguity means that it is infeasible to identify which nodes have generated the signature.

Definition 2: ($\mathcal{R}_n^1$ Signer Ambiguity) Let $L = \{y_0, \cdots, y_{n-1}\}$ be the set of public keys and each element is associated with a private key x_i, where each pair of keys is generated as $(x_i, y_i) \leftarrow \mathsf{Setup}(1^\ell)$. $\mathcal{R}_n^1$ possesses perfectly signer-ambiguity, if the following conditions are satisfied: For any L, any massage $M_r \in \mathcal{M}$, and any $\sigma \leftarrow \mathsf{RSign}_n^1(x, M_r, L)$, where $x \in \{x_0, \cdots, x_{n-1}\}$, given (L, M_r, σ), any unbound adversary $\mathcal{A}$ outputs j such that $x = x_j$ with probability $1/|L|$.
Here, by $A \leftarrow B$ we denote a uniform choice of an element from set B and its assignment to A.

Unforgeability for the ring signature schemes has been defined by Abe et al [2]. They utilized the notion of the existential unforgeability against adaptive chosen message attacks [13], where an adversary is given unbound access to the signing oracle and allowed to ask signatures for arbitrary messages. They also allow the adversary to choose arbitrary set of public keys as subset of initially considered set of public keys every time it accesses to the signing oracle.

Definition 3: ($\mathcal{R}_n^1$ - Existential Unforgeability against Adaptive Chosen Message Attacks (EU-ACPA)) Let $\sigma \leftarrow \mathsf{RSign}_n^1(x, M, L)$, where x is the signer's private key, $M \in \mathcal{M}$, L denotes the set of public keys, and σ is the resultant $\mathcal{R}_n^1$ signature. Let $\mathcal{R}_n^1$ be a signing oracle that takes any (M, L) as input and outputs a valid ring signature σ and $\mathsf{RVerify}_n^1(\sigma) = accept$. We say $\mathcal{R}_n^1$ is existentially unforgeable against adaptive chosen message attacks, if for any polynomial-time oracle $\mathcal{A}$ such that $\sigma \leftarrow \mathcal{A}(\mathcal{L}, \mathcal{R}_n^1)$, its output satisfies $\mathsf{RVerify}_n^1(\sigma, L) = accept$ only with negligible probability in ℓ, i.e.,

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EU\text{-}ACPA}}(\ell) = \ & \Pr[\sigma \leftarrow \mathcal{A}(\mathcal{L}, \mathcal{R}_n^1, M), \mathsf{RVerify}_n^1(\sigma, L) \\ & = accept] \leq \epsilon(\ell),\end{aligned}$$

where $\epsilon(\ell)$ is a negligible function.

Definition 4: $\mathcal{E}$ is an encryption scheme that is comprised of the following algorithms.

- $\mathcal{E}$-Setup: is a probabilistic algorithm that on input a security parameter ℓ, outputs definitions of the message space $\mathcal{M}_e$, the ciphertext space $\mathcal{C}$.
- Encrypt: is a probabilistic algorithm that takes as input $\langle \{A_j\}_{j \in \mathcal{S}_m}, M \rangle$, where $\{A_j\}_{j \in \mathcal{S}_m}$ are a list of m elements generated from RSign_n^1 and $M \in \mathcal{M}_e$, and outputs a ciphertext tuple $\langle C, b$, where C is the ciphertext and b is the corresponding parameter.
- Decrypt: is a deterministic algorithm that takes as input $\langle C, b, \{x_i\}_{i \in \mathcal{S}_m} \rangle$, where C is the ciphertext, b is the corresponding parameter, and $\{x_i\}_{i \in \mathcal{S}_m}$ is the set private keys used in generating the $\mathcal{R}_n^1$ signature.

$\mathcal{E}$ is based on the ElGamal encryption scheme whose security has been studied by Tsiounis and Yung [14]. They showed that ElGamal encryption scheme is as secure as the Diffie-Hellman Decisional problem. We require the $\mathcal{E}$ to be semantic secure [15]. We define security in terms of the sense of indistinguishability. Intuitively, if it is infeasible for an adversarial algorithm to distinguish between the encryption of any two messages, even if these messages are given, then the encryption is secure. Our scheme should be unforgeable against Indistinguishability (IND) and Adaptive Chosen Ciphertext (CCA2) [16]. It is easy to prove that ElGamal encryption is not secure against IND-CCA2. To make it secure against IND-CCA2, we adopt Schnorr-Jakobsson approach [17] to sign the encryption with the Schnorr signature scheme.

Definition 5: ($\mathcal{E}$ - Security against IND-CCA2) Let ($\mathcal{E}$-Setup, Encrypt, Decrypt) be an $\mathcal{E}$ encryption scheme. We say $\mathcal{E}$ is secure against IND-CCA2, if there exists no polynomial-time adversarial oracle $\mathcal{A}$ that on input a ciphertext and the public key outputs the original message or on input the public key outputs the secret key.

IV. The Scheme

We now give a concrete $\mathcal{R}_n^1$ signature scheme by following our definitions by modifying Abe-Ohkubo-Suzuki ring signature scheme [2].

A. The $\mathcal{R}_n^1$ Scheme

We describe the concrete $\mathcal{R}_n^1$ scheme. In this scheme, when a ring signature is constructed, the signers also prove the knowledge of the private keys that have been embedded in the ring signature. In the presentation, we will omit the modulo, when it is clear for the context.

- $\mathcal{R}$-Setup: On input a security parameter ℓ, select a prime p, which is published along with $g \in \mathbb{Z}_p^*$ of order $q | p - 1$. The spaces $\mathcal{S}_r, \mathcal{M}$ are defined as follows: $\mathcal{S}_r = \mathbb{Z}_q$, $\mathcal{M} = \mathcal{M}$. two cryptographic functions $H : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $\tilde{H} : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ are also selected. Private keys $x_i, 0 \leq i \leq n-1$ for the ring, are selected uniformly at random from $\mathbb{Z}_q$. The public keys are computed as $L = \{y_i = g^{x_i} \bmod p\}$ and are made public.

- RSign_n^1: The algorithm takes as input $\langle \{x_i\}_{i \in \mathcal{S}_m}, L, M_r \rangle$, where $\mathcal{S}_m$ lists the set of indices of the ring signature signers, L denotes public keys of all parties in the ring, and $M_r \in \mathcal{M}$ is a message. Algorithm then computes $\tilde{g} = \tilde{H}(L, M_r, T)$, where T denotes a concatenation of time and date. Let $\mathcal{S}_m$ be the set of private keys used to sign.
  - Initialization: Select $a_j \in_R \mathbb{Z}_q$, $j \in \mathcal{S}_m$ and compute:

    $$c_{k+1} = H_{k+1}(L \| M_r \| g \| \tilde{g} \| \{g^{a_j} \| \tilde{g}^{a_j}\}_{j \in \mathcal{S}_m}),$$

    where $\|$ denotes a bitwise concatenation and $\{A(j) \| B(j)\}_{j \in \mathcal{S}_m}$ denotes m bitwise concatenations with respect to $A(j) \| B(j)$ and $j \in \mathcal{S}_m$.
  - Forward sequence: For $i = k+1, \cdots, n-1, 0, 1, \cdots, k-1$ and $j \in \mathcal{S}_m$, select $s_{i,j} \in_R \mathbb{Z}_q$, and compute

    $$c_{i+1} = H_{i+1}(L \| M_r \| g \| \tilde{g} \| \{e_i^{(j)} \| \tilde{e}_i^{(j)}\}_{j \in \mathcal{S}_m}),$$

    where $e_i^{(j)} = g^{s_{i,j}} y_{i,j}^{c_i}$ and $\tilde{e}_i^{(j)} = \tilde{g}^{s_{i,j}} A_j^{c_i}$. A_j is computed as $A_j = \tilde{g}^{x_j}$, $j \in \mathcal{S}_m$.
  - Forming the ring: Compute $s_{k,j} = a_j - x_{k,j} c_k$, for $j \in \mathcal{S}_m$.

  The algorithm outputs

  $$\sigma = (c_0, \{s_{0,j}, \cdots, s_{n-1,j}\}, A_j, M_r).$$

  The R_n^1 signature is then forwarded to the receiver.

- $\mathsf{RVerify}_n^1$: The algorithm takes as input $\langle \sigma, L \rangle$, where $\sigma = \langle c_0, \{s_{0,j}, \cdots, s_{n-1,j}\}, A_j, M_r \rangle$ and L denotes all public keys of the ring. it computes:

  $$c_{i+1} = H_{i+1}(L \| M_r \| g \| \tilde{g} \| e_i^{(j)} \| \tilde{e}_i^{(j)}).$$

  where $e_i^{(j)} = g^{s_{i,j}} y_{i,j}^{c_i}$ and $\tilde{e_i}^{(j)} = \tilde{g}^{s_{i,j}} A_j^{c_i}$. Accept, if

  $$c_0 = H_0(L \| M_r \| g \| \tilde{g} \| e_{n-1}^{(j)} \| \tilde{e}_{n-1}^{(j)}).$$

In the above scheme, the signers intend to achieve two goals in the ring signature signing: (1) Signing a message $M_r \in \mathcal{M}$, and (2) Proving the following discrete logs equalities:

$$\log_g y_j = \log_{\tilde{g}} A_j, \quad j \in \mathcal{S}_m.$$

The proof algorithm embedded in the ring signature signing is based on the Chaum-Pedersen proof of equality of discrete logs [18].

If $\mathsf{RVerify}_n^1$ outputs *accept*, then he can implement the $\mathcal{E}$ algorithm. He has the choice of either sending a message to the ring or alternatively sending m messages to the ring. In the former case, he is sure that the nodes in $\mathcal{S}_m$ can collaboratively retrieve the message. In the later case, each node in $\mathcal{S}_m$ can retrieve a message from the m messages sent by the encrypter.

- $\mathcal{E}$-Setup: On input security parameter ℓ, select a prime p, which is published along with $g \in \mathbb{Z}_p^*$ of order $q|p-1$. Select the message/ciphertext space $\mathcal{M}_e = \mathcal{C} = \mathbb{Z}_p^*$.
- Encrypt: Take as input $\langle A_j, M \rangle$, where A_j is obtained from the original $\mathcal{R}_n^1$ signature and $M \in \mathbb{Z}_p^*$, choose a random $r \in \mathbb{Z}_q$, and compute

  $$K_j = A_j^r, \quad b_j = \tilde{g}_k^r,$$
  $$C = MK_j.$$

  Output $\langle C, b_j \rangle$. To achieve security against CCA2, C should be signed by the sender. Here, we omit it without losing generality of the scheme.
  Alternatively, the sender can send m messages to the ring. Choose $M \in \{0,1\}^*$, and compute

  $$C = MK_j \bmod p.$$

  Output $\{C, b_j\}$.
- Decrypt: Taking as input

  $$\langle C, A_j, b_j \rangle,$$

  the corresponding node encrypts:

  $$C/b_j^{x_j} = M \bmod p.$$

Theorem 1: The $\mathcal{R}_n^1$ scheme is correct.
Proof: We show that the ring for a ring signature is perfectly closed.

$$\begin{array}{rcl}
c_{k+1} & = & H_{k+1}(L\|M_r\|g\|\tilde{g}\|g^a\|\tilde{g}^a) \\
c_{k+2} & = & H_{k+2}(L\|M_r\|g\|\tilde{g}\|g^{s_{k+1}}y_{k+1}^{c_{k+1}}\|\tilde{g}^{s_{k+1}}A_j^{c_{k+1}}) \\
 & & \ldots \\
c_n & = & H_n(L\|M_r\|g\|\tilde{g}\|g^{s_{n-1}}y_{n-1}^{c_{n-1}}\|\tilde{g}^{s_{n-1}}A_j^{c_{n-1}}) = c_0 \\
 & & \ldots \\
c_{k+1} & = & H_{k+1}(L\|M_r\|g\|\tilde{g}\|g^{s_k}y_k^{c_k}\|\tilde{g}^{s_k}A_j^{c_k}) \\
 & = & H_{k+1}(L\|M_r\|g\|\tilde{g}\|g^a\|\tilde{g}^a)
\end{array}$$

The proof of equality of multiple discrete logs are based on the scheme due to Chaum and Pedersen [18]. The proof can be reduced to the following proof. Given $y = g^x$, $A = \tilde{g}^x$, prove $\log_g y = \log_{\tilde{g}} A$ by zero knowledge. Select at random $a \in \mathbb{Z}_q$ and compute $s = a - cx$, where $c = H(g\|\tilde{g}\|g^s y^c\|\tilde{g}^s A^c)$. The proof output is (c, s). The verification is done by verifying the equality of $c = H(g\|\tilde{g}\|g^s y^c\|\tilde{g}^s A^c)$. □

Theorem 2: The $\mathcal{R}_n^1$ scheme provides certainty to the number of signers in the ring.
Proof (Sketch) : The proof of equalities of $\log_g y_j = \log_{\tilde{g}} A_j, j \in \mathcal{S}_m$ ensures that only there nodes in $\mathcal{S}_m$ have be involved in the signing. Only those nodes can collaboratively seal the ring with $s_{k,j} = a_j - x_{k,j}c_k$, $j \in \mathcal{S}_m$. □

Theorem 3: The $\mathcal{R}_n^1$ Provides Signer Ambiguity.
Proof (Sketch) : We has shown in Theorem 2 that the number of signers for a ring signature is certain. The scheme still is signer-ambiguous. All s_i are randomly selected from $\mathbb{Z}_q$ except $\{s_j\}_{j \in \mathcal{S}_m}$ at the closing point. For fixed (L, M_r), $\{s_i\}$ has q^n. Note that a_j are uniformly chosen from $\mathbb{Z}_q$ variations regardless the closing point. □

The security of the scheme is proven in the random oracle model. We assume that all hash functions are the same and are treated as a random oracle and RSign is treated as a signing oracle. Let $\mathcal{A}$ be a (t, ϵ, q_h)-adversary that requests accesses the random oracle q_h times. and output a forged the signature (L, M, σ) with probability at least ϵ and running time at most t.

Theorem 4: If there exists (t, ϵ, q_h)-adversary $\mathcal{A}$ for public keys L of n, then there exists a simulator (τ, μ)-SIM that takes advantage of $\mathcal{A}$ to compute discrete log x_k of $(p, q, y_k, g) \in L$ and A_k with probability at least μ within running time τ, for $\tau < 2/\epsilon$ and $\mu > \frac{9}{25}$ under condition that $\epsilon > \frac{q_h}{qp}$.
Proof: We consider only a single node case ($m = 1$). It is easy to extend it to multiple nodes. SIM simulates the random oracles that is associated with the signing oracle and each hash function. The signing oracle takes as input (L, M) to sign. The random oracle take as input $Q(j, L_j, M_j, r_j, r_j')$ and outputs $H(L_j\|M_j\|r_j\|r_j')$. The system is simulated in terms of the following experiment Exp.

```
select $a \in \mathbb{Z}_q$, $A \in \mathbb{Z}_p^*$;
compute $\tilde{g}_i = H_i(L_j\|M_j\|T)$
compute $c_0 = H(L_j\|M_j\|g^a\|\tilde{g}^a)$;
for ($i = 0; i <= n_j - 1; i$++)
    compute $e_i = g_i^{s_i} y_i^{c_i}$ and $e_i' = \tilde{g}_i^{s_i} A^{c_i}$;
if $i \neq n_j - 1$, then
    compute $c_{i+1} = H_{i+1}(L_j\|M_j\|e_i\|e_i')$;
compare $c_0$ with $H_0(L_j\|M_j\|e_{n_j-1}\|e_{n_j-1}')$;
```

Here, $n_j = |L_j|$. If c_0 is equal to $H_0(L_j\|M_j\|e_{n_j-1}\|e_{n_j-1}')$ and $\log_{\tilde{g}} A = \log_g y_{n-1}$, the experiment successes; otherwise, fails. For a success, Exp outputs s_{n_j-1} which is equal to $a - x_{n-1}c_{n_j-1}$. Since the last step in the experiment determines the result, for simplicity, we assume that q_h is the number of times accessing the hash oracle in the last step and omit other queries. The probability of success for (t, ϵ, q_h)-adversary $\mathcal{A}$ running an Exp is at least $\epsilon = \frac{q_h}{qp}$. $\mathcal{A}$ runs Exp $t_1 = 1/\epsilon$ times. The probability of finding a valid s and A is at least

$$1 - (1 - \epsilon)^{1/\epsilon} \approx 1 - e^{-1} > 3/5.$$

$\mathcal{A}$ then runs Exp $t_2 = t_1$ times again by using a different input (L_j, M') with $(L_j, a, g, \tilde{g})$ unchanged. Exp outputs s' such that $s' = a - x_{n_j-1}c_{n_j-1}'$ with probability 3/5. x_{n_j-1}

can then be computed $x_{n_j-1} = \frac{s-s'}{c_{n_j-1}-c'_{n_j-1}}$. The total times used for the simulation is up to $t_1+t_2 = \frac{2qp}{q_h}$ with probability $\mu > \frac{9}{25}$. □

V. Conclusion

We proposed a novel ring signature scheme for anonymous MANET communications. It provides the following features: (1) The signing node can be authenticated by other nodes without revealing its identity and (2) any node can send a message or messages to the node who has be authenticated. These features are not satisfied by the original ring signature scheme introduced by Abe *et al.*[2].

References

[1] A. Shamir, R. Rivest, and Y. Tauman, "How to leak secret," in *Advances in Cryptology–ASIACRYPT 2001,* LNCS 2248. Springer-Verlag, Berlin, 2001, pp. 552–565.

[2] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in *Advances in Cryptology–ASIACRYPT 2002,* LNCS 2501. Springer-Verlag, Berlin, 2002, pp. 415–432.

[3] D. Chaum and E. van Heijst, "Group signatures," in *Advances in Cryptology, Proc. EUROCRYPT 91,* LNCS 547. Springer-Verlag, 1991, pp. 257–265.

[4] L. Chen and T. P. Pedersen, "New group signature schemes," in *Adances in cryptology - EUROCRYPT'94, Lecture Notes in Computer Secience 950.* Springer-Verlag, Berlin, 1994, pp. 171–181.

[5] J. Camenisch, "Efficient and generalized group signatures," in *Adances in cryptology - EUROCRYPT'97, Lecture Notes in Computer Secience 1233.* Springer-Verlag, Berlin, 1997, pp. 465–479.

[6] J. Camenisch and M. Michels, "A group signature scheme with improved efficiency," in *Advances in Cryptology–ASIACRYPT'98,* LNCS 1514. Springer-Verlag, Berlin, 1998, pp. 160–174.

[7] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Advances in Cryptology, Proc. CRYPTO 97,* LNCS 1296. Springer-Verlag, Berlin, 1997, pp. 410–424.

[8] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology, Proc. CRYPTO 2004,* LNCS 3152. Springer-Verlag, Berlin, 2004, pp. 56–75.

[9] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings." Springer-Verlag, 2003, pp. 533–547.

[10] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM,* vol. 24, no. 2, pp. 84–88, 1981.

[11] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Information Security and Privacy–ACISP 2004,* LNCS 3108. Springer Verlag, 2004, pp. 325–335.

[12] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Advances in Cryptology, Proc. CRYPTO 2002,* LNCS 2442. Springer Verlag, 2002, pp. 465–480.

[13] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[14] T. Tsiounis and M. Yung, "On the security of ElGamal based encryption." Springer Verlag, 1998, pp. 117–135.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, April 1984.

[16] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in *Advances in Cryptology, Proc. CRYPTO 98,* LNCS 1462, H. Krawczyk, Ed. Springer Verlag, 1998, pp. 26–46.

[17] C. P. Schnorr and M. Jakobsson, "Security of signed elgamal encryption," T. Okamoto, Ed. Springer Verlag, 2000, pp. 73–89.

[18] D. Chaum and T. P. Pedersen, "Wallet databases with observers," in *Advances in Cryptology – CRYPTO '92 Proceedings*. Springer-Verlag, 1992, pp. 89–105.