Application of Identity-Based Cryptography in Mobile Ad Hoc Networks

Shushan Zhao
Computer Science Department
University of Windsor

This is a survey on application of Identity-Based Cryptography in mobile ad hoc networks. In this survey, we review all papers that are available in the literature on security schemes on mobile ad hoc networks using Identity-Based Cryptography during years 2001 to 2007. To introduce the topic, we first review most important developments on general Identity-Based Cryptography. The survey introduces briefly the technology of Identity-Based Cryptography, summarizes different approaches of applying it to secure mobile ad hoc networks. It also discusses future directions and open problems of general Identity-Based Cryptography and its application in mobile ad hoc networks.

Categories and Subject Descriptors: X.x.x [**Security**]: Network, Cryptography—*documentation*

Additional Key Words and Phrases: Identity-based, cryptography, MANET,

Contents

1. INTRODUCTION

Research on Mobile Ad hoc NETworks (MANETs) has been conducted for almost 20 years. Research on security of MANETs follows the research on MANETs from the beginning, and is still very active in research communities and in industry. During these years, a large number of papers have been published on the topic of security of MANETs. The research topic has continued to be active for so long because of the certain characteristics of MANETs and the special challenges these characteristics impose on it. We will discuss these characteristics and challenges shortly.

Since 2001, Identity-Based Cryptography (IBC) has been getting more and more attention from researchers on security, including security of MANETs. IBC is a special form of Public Key Cryptography (PKC). Some properties of IBC make it especially suitable for MANETs as will be shown shortly. In this survey, we study the application of IBC in the area of security of MANETs. As preliminaries, we first review most important development on general IBC schemes itself.

The scope of this study is confined to research papers published in formal conferences proceedings and journals. The papers were identified by searching in ACM, IEEE, LNCS online repositories. For completeness, we also study some other papers to which the authors of the original papers make reference. As a result, we select 8 papers out of about 100 published in the area of general "Identity-Based Cryptography". We only select those that we think are of great importance to the area of security of MANETs. We study 29 papers in the area of "security of MANETs based on IBC" from 1979 to 2007, which seem to be all the published papers in this area. Besides, we refer to about 40 other publications, including books, theses, and papers, for background information.

Through this study, we introduce the development of general IBC technology and its application in security of MANETs. We also identify future directions and open questions on this topic.

The survey is organized as follows: Section 2 briefly reviews the background of research on security of MANETs and Identity-Based Cryptography. Section 3 reviews and summarizes important papers in the development of general IBC which have had a great influence on security of MANETs. Section 4 reviews and summarizes papers applying IBC in MANETs, in sub-areas of key management, PKIs, secure communications, secure routing, and other miscellaneous uses. Section 5 summarizes the survey by presenting open questions and future directions of applying IBC to secure MANETs.

2. BACKGROUND

2.1 Background of Research on Security of MANETs

Research on MANET security is still in its early stage. Various security mechanisms have been proposed, widely used, and proven to be effective in wired networks, but no single mechanism provides all the services required in a MANET. Due to certain characteristics of MANETs, some security mechanisms are not applicable to this environment. These certain characteristics of ad hoc networks include: lack of a network infrastructure and online administration, the dynamics of the network topology and node membership, the potential attacks from inside the network, and

vulnerability of wireless links.

Existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Different solutions have been proposed to address attacks in different layers. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks [Yang et al. 2004].

Many security countermeasures are achieved by the use of cryptography. A variety of cryptography technologies have been used. Cryptography technologies used in MANETs can be classified into two categories: *Symmetric Key based*, and *Asymmetric Key based* [Zhou and Haas 1999]. In symmetric cryptography, if an attacker compromises the symmetric key of a group of users, then all encrypted messages for that group will be compromised. Whereas in asymmetric cryptography, although compromise of a private key of a user does not reveal messages encrypted for other users in the group, it is nevertheless computationally expensive. Asymmetric cryptography technologies rely on a public key infrastructure (PKI). The success of PKI depends on the availability and security of a Certificate Authority (CA). Thus, a PKI requires a central control point, which everybody trusts. The difficulty in applying a PKI in a MANET is that such a central control point is not feasible. Even if it is deployed, it cannot be well protected and would become the most vulnerable point in the system. There are several research directions for solving this problem. One is to retain the certificate authority concept, but distribute its functionality into multiple servers or trusted nodes. In this way, both the availability and the security of the CA can be improved [Zhou and Haas 1999]. Another approach is to discard the centralized CA, and instead, create a completely distributed and self-organized key management system, e.g. the PGP scheme [Hubaux et al. 2001]. Identity-Based cryptography is a new approach to eliminate the requirement of a CA and even public key certificates (PKCs).

2.2 A Brief History of Identity-Based Cryptography

Identity-Based cryptography schemes are in the category of "*Asymmetric Key based*" cryptography. Identity-Based cryptography specifies a cryptosystem in which both public and private keys are based on the identities of the users. The idea of Identity-Based cryptography was first proposed by Shamir [Shamir 1984]. Such a scheme has the property that a user's public key is an easily calculated function of his identity, while a user's private key can be calculated for him by a trusted authority, called Private Key Generator (PKG). The Identity-Based public key cryptosystem can be an alternative for certificate-based PKI, especially when efficient key management and moderate security are required. Compared to traditional PKI, it saves storage and transmission of public keys and certificates, which is especially attractive for devices forming MANETs. Thus, application of Identity-Based cryptography in MANETs is an important research topic in areas of both cryptography and MANETs.

For a long time after Shamir published his idea, the development on Identity-Based cryptography was very slow. Desmedt and Quisquater [Desmedt and Quisquater], Tanaka [Tanaka 1987], Tsujii and Itoh [Tsujii and Itoh 1989], Maurer and Yacobi [Maurer and Yacobi 1991] etc. conducted research on this topic and made

some interim developments. Joux [Joux 2000], in 2000, showed that Weil pairing can be used for "good" by using it in a protocol to construct three-party one-round Diffie-Hellman key aggrement. This was one of the breakthroughs in key agreement protocols. After this, Boneh and Franklin [Boneh and Franklin 2001] presented in Crypto 2001 an Identity-Based encryption scheme based on properties of bilinear pairings on elliptic curves which is the first fully functional, efficient and provably secure Identity-Based encryption scheme. In Asiacrypt 2001, Boneh, Lynn and Shacham proposed a basic signature scheme using pairing, the BLS scheme [Boneh et al. 2001], that has the shortest length among signature schemes in classical cryptography.

Subsequently numerous cryptographic schemes based on the work of [Boneh and Franklin 2001] and [Boneh et al. 2001] were proposed. There are also a few Identity-Based cryptographic schemes using other approaches, for example, Cocks' scheme is based on the quadratic residuosity problem [Cocks 2001]. In this survey, we focus on schemes using pairing, which are the mainstream in Identity-Based cryptography.

2.3 Preliminaries of Identity-Based Cryptography

Following Boneh and Frankin's scheme [Boneh and Franklin 2001], Identity-Based cryptographic schemes are mostly built on a *Bilinear Map* over elliptic curves. A *Bilinear Map* is denoted $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ between two cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ of order q for some large prime q, where $\mathbb{G}_1$ is the group of points of an elliptic curve over $\mathbb{F}_p$ and $\mathbb{G}_2$ is a subgroup of $\mathbb{F}^*_{p^2}$.

A cryptographic bilinear map satisfies the following properties [Dutta et al. 2004, pp 6]:

(1) **Bilinear**: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}^*_q$ [1]. This can be restated in the following way. For $P, Q, R \in \mathbb{G}_1, \hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$ and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$.

(2) **Non-degenerate**: $\hat{e}(P, P) \in \mathbb{F}_{p^2}$ is an element of order q, and in fact a generator of $\mathbb{G}_2$. In other words, $\hat{e}(P, P) \neq 1$

(3) **Computable**: Given $P, Q \in \mathbb{G}_1$ there is an efficient algorithm to compute $\hat{e}(P, Q)$.

Modified Weil Pairing and Tate Pairing are examples of cryptographic bilinear maps. Currently, active research is being carried out to obtain efficient algorithms to compute pairings.

All Identity-Based cryptographic schemes are based on assumptions of hard problems. Mostly used assumptions are [Dutta et al. 2004, pp 7]:

—**Computational Diffie-Hellman (CDH) problem in** $\mathbb{G}_1$: there is no efficient algorithm to compute $\hat{e}(P, P)^{ab}$ from $P, aP, bP \in \mathbb{G}_1$ for $a, b \in \mathbb{Z}^*_q$.

—**Decisional Diffie-Hellman (DDH) problem in** $\mathbb{G}_1$: there is no efficient algorithm to decide if $c = ab \bmod q$ given P, aP, bP, cP for $a, b, c \in \mathbb{Z}^*_q$

[1] $\mathbb{Z}^*_q$ is the multiplicative group of integers modulo q. In particular, if q is a prime, $\mathbb{Z}^*_q = \{a | 1 \leq a \leq q - 1\}$

—**Weak Diffie-Hellman (W-DH) problem in** $\mathbb{G}_1$: there is no efficient algorithm to compute sQ from $P, Q, sP \in \mathbb{G}_1$ and $s \in \mathbb{Z}_q^*$. (W-DH problem is no harder than CDH problem).

—**Gap Diffie-Hellman (GDH) group**: A prime order group $\mathbb{G}_1$ is a GDH group if there exists an efficient polynomial-time algorithm which solves the DDH problem in $\mathbb{G}_1$ and there is no probabilistic polynomial-time algorithm which solves the CDH problem with non-negligible probability of success. The domains of bilinear pairings provide examples of GDH groups.

—**Bilinear Diffie-Hellman (BDH) problem in** $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$: there is no efficient algorithm to compute $\hat{e}(P, P)^{abc} \in \mathbb{G}_2$ from $P, aP, bP, cP \in \mathbb{G}_1$ where $a, b, c \in \mathbb{Z}_q^*$.

—**Decisional Bilinear Diffie-Hellman (DBDH) problem in** $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$: there is no efficient algorithm to decide if $r = \hat{e}(P, P)^{abc}$ given $r \in_R \mathbb{G}_2$ and $a, b, c \in_R \mathbb{Z}_q^*$

Unless otherwise stated, in following sections we use the same denotations as in this section, which are summarized in Table I:

Symbols	**Meanings**
$\mathbb{Z}$	set of integers
$\mathbb{Z}_n$	set of integers mod n
$\mathbb{F}_q$	the finite field with q elements
$E/\mathbb{F}_p$	elliptic curve over $\mathbb{F}_p$
$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$	a bilinear map between two cyclic groups $\mathbb{G}_1, \mathbb{G}_2$
P	an arbitrary point in $E/\mathbb{F}_p$
Q_{ID}	a point in $E/\mathbb{F}_p$ mapped from ID
d_{ID}	private key of ID
s	master secret key
P_{pub}	system public key
$/* \ldots\ldots */$	comments

Table I. Denotations used in this survey

3. IMPORTANT DEVELOPMENTS OF IDENTITY-BASED CRYPTOGRAPHY

Identity-Based cryptography has only a short history, so there are not many publications in the literature on this topic. We select the most important ones that have influence on the security of ad hoc networks, and study them in this survey.

3.1 The Concept of Identiy-based Cryptography

In 1984, Shamir introduced a novel type of cryptographic scheme, so-called Identity-Based cryptosystem, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party [Shamir 1984].

Shamir stated that "The scheme is based on a public key cryptosystem with an extra twist: instead of generating a random pair of public/secret keys and publishing one of these keys, the user chooses his name and network address as his public key. Any combination of name, social security number, street address, office number or telephone number can be used provided that it uniquely identifies the

user in a way he cannot later deny, and that it is readily available to the other party. The corresponding secret key is computed by a key generation center (PKG) and issued to the user when he first joins the network." Figure 1 illustrates his idea.

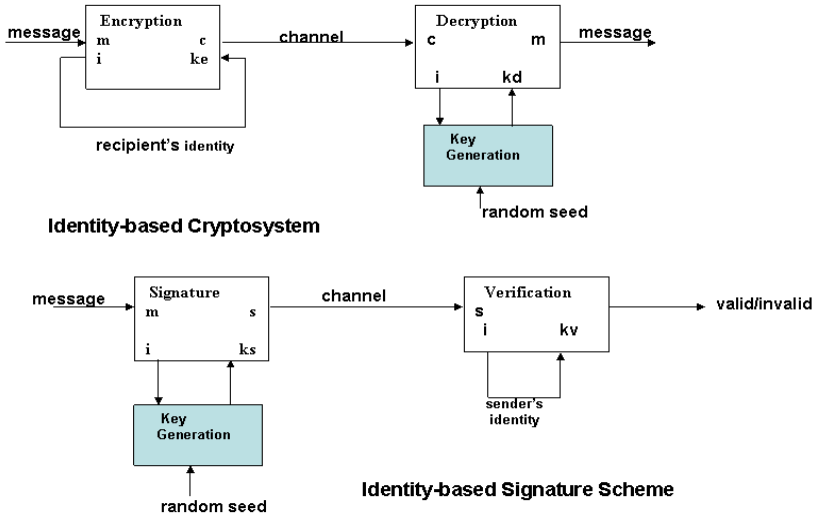

Fig. 1. Shamir's Identity-Based Cryptosystem and Signature Scheme ([Shamir 1984, pp 52])

In his paper, Shamir specifies the requirements of an implementation of such a scheme and lists the implementation principals:

—(a) The choice of keys is based on a truly random seed k. When the seed k is known, secret keys can be easily computed for a non-negligible fraction of the possible public keys.

—(b) The problem of computing the seed k from specific public/secret key pairs generated with this k is intractable .

Based on these requirements, he states that RSA scheme is not capable for such a scheme.

He states at that stage they have concrete implementation proposals only for Identity-Based signature schemes, but conjecture that such cryptosystems exist and encourage the readers to look for such systems.

3.2 Identiy-based Encryption Schemes

3.2.1 *The First Fully Functional Identiy-based Encryption Scheme.* The first fully functional scheme for Identity-Based Encryption is Boneh and Franklin's scheme published in [Boneh and Franklin 2001]. The authors refer to Shamir's idea about an Identity-Based Encryption (IBE) scheme [Shamir 1984], and several proposals for IBE schemes [Desmedt and Quisquater ; Tanaka 1987; Tsujii and Itoh 1989; Maurer and Yacobi 1991]. They consider none of them fully satisfactory, due to unrealistic requirements, such as users not colluding, long time for private key generation, or tamper-resistant hardware.

The security of their system is based on the Weil Diffie-Hellman Assumption (WDH), a natural analogue of the computational Diffie-Hellman assumption on elliptic curves. They build the IBE system from a bilinear map. They use the Weil pairing on elliptic curves as an example of such a map.

Their scheme is specified by four randomized algorithms [Boneh and Franklin 2001, pp 215]:

—Setup: They provide algorithms to map arbitrary string ID to pints on an elliptic curve. Set the system public key P_{pub} as sP where s is a random number in $\mathbb{Z}_q^*$, and P is an arbitrary point in $E/\mathbb{F}_p$ of order q. Choose a cryptographic hash function $H : \mathbb{F}_{p^2} \rightarrow \{0,1\}^n$ for some n. Choose a cryptographic hash function $G : \{0,1\}^* \rightarrow \mathbb{F}_p$. The system parameters are $params = \langle p, n, P, P_{pub}, G, H\rangle$. The master-key is $s \in \mathbb{Z}_q$.

—Extract: For a given string $ID \in \{0,1\}^*$ the algorithm builds a private key d_{ID} as $d_{ID} = sQ_{ID}$ where Q_{ID} is a point in $E/\mathbb{F}_p$ mapped from ID.

—Encrypt: Choose a random $r \in \mathbb{Z}_q$, and set the ciphertext to be $C = \langle rP, M \oplus H(g_{ID}^r)\rangle$ where $g_{ID} = \hat{e}(Q_{ID}, P_{pub}) \in \mathbb{F}_{p^2}$

—Decrypt: Let $C = \langle U, V\rangle$ be a ciphertext encrypted using the public key of ID, decrypt C using the private key d_{ID}: $V \oplus H(\hat{e}(d_{ID}, U)) = M$

Further, they analyze the security of their scheme, and state the scheme has chosen ciphertext security in the random oracle model assuming Weil Diffie-Hellman.

The scheme proposed in this paper is later referred and improved by follow-up researchers for many times, and widely adopted in many ID-Based security schemes.

3.2.2 *Authenticated Identiy-based Encryption Schemes.* In Boneh and Franklin's IBE system [Boneh and Franklin 2001], encryption and decryption are not authenticated. Lynn identifies this problem in [Lynn 2002], and identifies the requirement for a system that has authentication but not nonrepudiation. On the basis of the work of [Boneh and Franklin 2001], the author proposes a method for integrating authentication with encryption in the Boneh-Franklin IBE system.

His scheme changes the encrypt and decrypt algorithms of [Boneh and Franklin 2001] by involving the sender's private key and the receiver's identity in the so-called *Authenticated-Encrypt* algorithm, and the sender's identity and the receiver's private key in the so-called *Authenticated-Decrypt* algorithm.

—**Authenticated-Encrypt**: Assume A sends message M to B. A chooses a random $\sigma \leftarrow \{0,1\}^n$, computes $r = H_3(\sigma, M)$ and $s := e(d_A, H_2(ID_B))$ and outputs the ciphertext $C := \langle r, \sigma \oplus H_1(r,s), E_{H_4(\sigma)}(M)\rangle$, where $H_1 : \mathbb{F}_q \times \mathbb{G}_2 \rightarrow$

$\{0,1\}^n$, $H_2 : \{0,1\}^* \to \mathbb{G}_1$, $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{F}_q$, $H_4 : \{0,1\}^n \to \{0,1\}^n$, E_K is a secure symmetric cryptosystem encryption function.

—**Authenticated-Decrypt**: For a ciphertext $\langle U, V, W\rangle$, an ID ID_A, a private key d_B computer $s := \hat{e}(H_2(ID_A), d_B)$, $\sigma := V \oplus H_1(U, s)$, $M := D_{H_4(\sigma)}(W)$, where D_K is a secure symmetric cryptosystem decryption function.

The author proves the security of this scheme, and shows that it is secure and authenticated using only the BDH assumption and the random oracle model.

3.2.3 *Hierarchical Identiy-based Encryption Schemes.* In a large network, the PKG in IBE schemes would have a burdensome job. One solution to this problem is to allow a hierarchy of PKGs in which the PKGs have to compute private keys only for the entities immediately below them in the hierarchy. Some Hierarchical Identity-Based Encryption (HIBE) schemes have been proposed.

In [Boneh et al. 2005], the authors first review previous HIBE systems [Gentry and Silverberg 2002; Boneh and Boyen 2004], and identify a problem with them: the length of ciphertexts and private keys, as well as the time needed for decryption and encryption, grows linearly in the depth l of the hierarchy. They present a HIBE system where the ciphertext size as well as the decryption cost are independent of the hierarchy depth l.

In their scheme, identities are vectors: a vector of dimension k represents an identity at depth k. The system has four algorithms [Boneh et al. 2005, pp 445]:

—Setup: Assume $\mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$, $\mathbb{G}$ and $\mathbb{G}_1$ are two multiplicative cyclic groups. A Trusted Authority (TA) selects a random generator $g \in \mathbb{G}$, a random $\alpha \in \mathbb{Z}_p$, and set $g_1 = g^\alpha$, random elements $g_2, g_3, h_1, \ldots\ h_l \in \mathbb{G}$. The public parameters are $\langle g, g_1, g_2, g_3, h_1, \ldots\ h_l\rangle$, and the master key is g_2^α

—KeyGen: *KeyGen* takes as input an identity $ID = (I_1, ..., I_k)$ at depth k and the private key $d_{ID|k-1}$ of the parent identity $ID_{|k-1} = (I_1, ..., I_{k-1})$ at depth $k-1$, and then outputs the private key d_{ID} for identity ID. $d_{ID|k-1} = (g_2^\alpha \cdot (h_1^{I_1} \cdots h_{k-1}^{I_{k-1}} \cdot g_3)^{r'}, g^{r'}, h_k^{r'}, ..., h_l^{r'}) = (a_0, a_1, b_k, ...b_l)$. To generate d_{ID}, *KeyGen* picks a random $t \in \mathbb{Z}_p$ and outputs $d_{ID} = (a_0 \cdot b_k^{I_k} \cdot (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^t, a_1 \cdot g^t, b_{k+1} \cdot h_{k+1}^t, ..., b_l \cdot h_l^t)$. Let $r = r' + t \in \mathbb{Z}_p$, then $d_{ID} = (g_2^\alpha \cdot (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^r, g^r, h_{k+1}^r, ..., h_l^r)$.

—Encrypt: To encrypt a message $M \in \mathbb{G}_1$ under the public key $ID = (I_1, ..., I_k) \in (\mathbb{Z}_p^*)^k$, *Encrypt* picks a random $s \in \mathbb{Z}_p$ and outputs $CT = (\hat{e}(g_1, g_2)^s \cdot M, g^s, (h_1^{I_1} \cdot \cdots h_k^{I_k} \cdot g_3)^s) \in \mathbb{G}_1 \times \mathbb{G}^2$.

—Decrypt: Consider an identity $ID = (I_1, ..., I_k)$. To decrypt a given ciphertext $CT = (A, B, C)$ using the private key $d_{ID} = (a_0, a_1, b_{k+1}..., b_l)$, *Decrypt* outputs $A \cdot \frac{\hat{e}(a_1, C)}{\hat{e}(B, a_0)} = A \cdot \frac{\hat{e}(g^r, (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^s)}{\hat{e}(g^s, g_2^\alpha (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^r)} = \frac{A}{\hat{e}(g, g_2)^{s\alpha}} = M$

The authors analyze the efficiency and security of the scheme. They point out that the ciphertext contains only 3 elements and decryption takes only 2 pairings, while in previous HIBE systems, ciphertext size and decryption time grow linearly in the identity depth.Also, if $\hat{e}(g_1, g_2)$ is precomputed (or substituted for g_2 in the system parameters), encryption does not require any pairings. They notice the proof of full security (either in the random oracle or standard model) degrades

exponentially in the hierarchy depth. They state the same is true for all existing HIBE systems, and it is an open problem to construct a HIBE system where security does not degrade exponentially in the hierarchy depth.

3.2.4 *Multi-Decrypter Identiy-based Encryption Schemes.* Multi-Decrypter Encryption is also very useful in networking situations. Chai et al [Chai et al. 2007] identify the problem of low efficiency of multi-decrypter encryption using an ID-Based scheme. They refer to the work of [Shoup and Gennaro 2002; Baek and Zheng 2004], and review former solutions: group key, splitting-encrypting-concatenating, and multi-rounds encryption. They state the drawbacks of these solutions: less secure, long ciphertext, and high computational cost.

The authors propose a new multi-decrypter encryption scheme in the ID-based settings. In this scheme, the encrypter picks a random ephemeral key $r \in \mathbb{Z}_q$ and computes ciphertext for the message as a whole [Chai et al. 2007, pp 105]:

$$C = \langle U, V, W \rangle = \langle rP, rH_1(ID_1) + \cdots + rH_1(ID_n) + rQ, \hat{e}(P_{pub}, Q)^r M \rangle$$

One receiver can only partially decrypt the cyphertext, and generate a decryption share:

$$\delta_i = \hat{e}(U, d_{ID_i}) = \hat{e}(rP, sH_1(ID_i)) = \hat{e}(sP, rH_1(ID_i)) = \hat{e}(P_{pub}, rH_1(ID_i))$$

($Q \in_R \mathbb{G}$ is a system parameter.) To generate the plaintext, all the n decryption shares $\delta_i \in \mathbb{G}_1, i = 1, \cdots, n$ are required. A dealer (one of the receiver) computes:

$$\begin{aligned} W \prod_{i=1}^{n} \delta_i / \hat{e}(P_{pub}, V) &= W \prod_{i=1}^{n} \hat{e}(P_{pub}, rH_1(ID_i)) / \hat{e}(P_{pub}, rH_1(ID_1) + \cdots + rH_1(ID_n) + rQ) \\ &= \frac{W}{\hat{e}(P_{pub}, rQ)} = M \end{aligned}$$

The authors compare their scheme with former ones and point out the main advantages of their scheme: the number of pairing, multiplication and exoponentiation computation is dramatically reduced; the bit length is much shorter than former ones. The cost for the advantages is only one element longer than former schemes.

3.3 Identiy-based Signature Schemes

Based on Boneh and Franklin's IBE scheme [Boneh and Franklin 2001], Hess proposes an Identiy-based Signature Scheme in [Hess 2003]. He identifies the importance and requirement of a signature system matching Boneh and Franklin's IBE scheme. He suggests adding two algorithms to Boneh and Franklin's IBE scheme using the same *Setup* and *Extract* algorithms to provide signature and verification functions [Hess 2003, pp 312]:

—**Sign:** Given a secret key d_{ID} and a message $m \in 0, 1^*$, the signer chooses an arbitrary $P_1 \in \mathbb{G}_1$ and a random $k \in \mathbb{Z}_q^*$ and computes: $r = \hat{e}(P_1, P)^k$, $v = H(m, r)$, $u = vd_{ID} + kP_1$. The signature is then the pair $\langle u, v \rangle$.

—**Verify:** Given a public key Q_{ID}, a message m and a signature $\langle u', v' \rangle$, the verifier computes $r' = \hat{e}(u, P)\hat{e}(Q_{ID}, -P_{pub})^v$ /*= r*/, and accepts the signature if and only if $v' = H(m', r')$.

The author compares his scheme with previous ones such as [Paterson 2002; Sakai et al. 2000; Cha and Cheon 2003], and claims that his scheme is more computationally efficient. The author also discusses key escrow and the distribution of keys to multiple trust authorities.

3.4 Identiy-based Signcryption Schemes

In [Lynn 2002], the authors ask the question if there is a way to perform Identity-Based signcryption (Encryption-Signature) scheme using same system parameters and public and private keys. This question is answered by Boyen in [Boyen 2003]. In this paper the author refers to several proposed Identity-Based Encryption (IBE) schemes, such as [Boneh and Franklin 2001; Cocks 2001; Lynn 2002]; and Idenity-based signature (IBS) schemes, such as [Paterson 2002; Hess 2003; Cha and Cheon 2003]. He identifies the problem of lacking an algorithm that combines IBE and IBS in a practical and secure way. He suggests exploiting the similarities between IBE and IBS, and elaborates a dual-purpose IDB Encryption-Signature (IBSE) scheme based on a shared infrastructure, toward efficiency increases and security improvements.

The author presents an efficient IBSE construction. Using bilinear pairings and based on Boneh's work [Boneh and Franklin 2001], he adds two new algorithms: *Sign* that produces a signature for a given message and private key; *Verify* that checks the validity of a given signature for a given message and identity.

His scheme uses the properties of bilinear pairings to achieve a two-layer sign-then-encrypt combination, featuring a detachable randomized signature, followed by anonymous deterministic encryption. The main algorithms of this scheme are [Boyen 2003, pp 394]:

—*Sign:* A computes $j = Q_A^r, h = H_1(j, m), v = {d_A}^{r+h}$, where r is a random in $\mathbb{F}_p^*$, m is the message to be signed; outputs $\langle j, v\rangle$ as the signature, forwards $\langle m, r, ID_A, Q_A, d_A\rangle$ for *Encrypt*.

—*Encrypt:* A computes $u = \hat{e}(d_A, Q_B), k = H_3(u), x = j^k, w = u^{kr}, y = H_2(w) \oplus v, z = H_4(v) \oplus (ID_A, m)$; outputs the ciphertext $\langle x, y, z\rangle$

—*Decrypt:* Upon received ciphertext $\langle x', y', z'\rangle$, B computes $w' = \hat{e}(x', d_B)/* = \hat{e}(Q_A^{rk}, d_B)*/, v' = H_2(w') \oplus y'/* = v*/, (ID'_A, m') = H_4(v') \oplus z'/* = (ID_A, m)*/, u' = \hat{e}(Q_A, d_B)/* = u*/, k' = H_3(u')/* = k*/, j' = {x'}^{-k'}/* = j*/$, outputs $\langle m', j', v'\rangle$

—*Verify:* B computes $h' = H_1(j', m')$, and check whether $\hat{e}(P, v') \stackrel{?}{=} \hat{e}(sP, Q_A^{h'} \cdot j')$

The author has compared his scheme with other proposed schemes on a theorectical basis, and concludes that his scheme satisfies all the proposed security requirements, and yet is as compact as pairing-based IBE and IBS in isolation, offers detachable signatures, and supports multirecipient encryption with signature sharing for maximum scalability.

3.5 Key Generation Schemes of Identiy-based Cryptography

A basic key generation scheme of Identiy-based Cryptography has been present in [Boneh and Franklin 2001]. To scale to a large network of users and secure the key

generation process, some key generation schemes have been proposed. Boneh et al [Boneh et al. 2005] proposed a hierarchical key generation scheme.

Lee et al [Lee et al. 2004] propose a secure key generation scheme in Identity-Based cryptography. The authors identify the problem of key escrow and challenge of secure key issuing in Identity-Based cryptography. They refer to previous work on this topic and point out the drawback of each one: [Boneh and Franklin 2001] uses multiple authority approach which has the burden of multiple identification of user; Gentry et al [Gentry 2003] propose certificate-based encryption which loses the advantages of Identity-Based encryption; Al-Riyami et al [Al-Riyami and Paterson 2003] propose certificateless public key cryptography in which the self-generated public key cannot be verified by others.

The authors propose a new secure key issuing protocol in which a private key is issued by a key generation center (KGC) and then its privacy is protected by multiple key privacy authorities (KPAs). For all $i = 1, \cdots, n$, KPA_i chooses his master key s_i and computes his public key $P_i = s_i P$. Then KPAs cooperate sequentially to compute the system public key $Y = s_0 s_1 ... s_n P$.

A user ID gets its private key in three stages [Lee et al. 2004, pp 73]:

(1) In key issuing stage, a user with identity ID sends his identity ID and blinding factor $X = xP$ to the KGC and requests him to issue a partial private key. Then, after checking the identity of the user and computing the public key of the user – Q_{ID}, the KGC issues a partial private key to the user in a blinded manner: $Q'_0 = H_3(\hat{e}(s_0 X, P_0)) s_0 Q_{ID}$, together with a signature: $Sig_0(Q'_0) = s_0 Q'_0$. Here $H_3(\hat{e}(s_0 X, P_0))$ is a blinding factor; a secure channel between the user and the KGC. User can unblind it using his knowledge of x, since $H_3(\hat{e}(s_0 X, P_0)) = H_3(\hat{e}(s_0 xP, P_0)) = H_3(\hat{e}(P_0, P_0)^x)$.

(2) In key securing stage, the user requests multiple KPAs in a sequential manner to provide key privacy service by sending ID,X,Q'_{i-1} and $Sig_{i-1}(Q'_{i-1})$. Then KPAs return the private key shares: $Q'_i = H_3(\hat{e}(s_i X, Pi)) s_i Q'_{i-1}$ and signature $Sig_i(Q'_i) = s_i Q'_i$ in a blinded manner.

(3) Finally, in key retrieving stage, the user unblinds it to retrieve the real private key:$D_{ID} = \frac{Q'_n}{H_3(\hat{e}(P_0,P_0)^x) \cdots H_3(\hat{e}(P_n,P_n)^x)} = s_0 s_1 \cdots s_n Q_{ID}$. The user can verify the correctness of his private key by $\hat{e}(D_{ID}, P) = \hat{e}(Q_{ID}, Y)$.

The authors have analyzed the security of this scheme and state that since the private key of a user is computed cooperatively by the KGC and n KPAs, the privacy of user's private key is kept if at least one authority remains honest. Only the legitimate user who knows the blinding parameter can unblind the message to retrieve the private key. The authors claim that their secure key issuing protocol successfully overcomes the key escrow problem of Identity-Based cryptography, thus it can be applied to more complex applications satisfying stronger security requirements; the issued key is a real Identity-Based private key, thus it can be used with any Identity-Based cryptosystems such as encryptions, signatures, and key agreements, preserving the advantages of Identity-Based cryptography.

3.6 Summary

In this section, we have introduced the concept of Identity-Based cryptography, review important developments as of encryption schemes, signature schemes, signcryption schemes and key generation schemes. We summarize these developments and corresponding papers in the following Table II.

Year	**Author(s)**	**Title of Paper**	**Main Contribution(s)**
1984	Shamir	Identity-Based Cryptosystems and Signature Schemes	The paper introduces the concept of Identity-Based cryptosystems and signature schemes, and proposes the basic implementation idea about it.
2001	Boneh and Franklin	Identity-Based Encryption from the Weil Pairing	The paper proposes the firstly fully functionally Identity-Based encryption scheme with detailed algorithms.
2002	Lynn	Authenticated Identity-Based Encryption	The paper adds authentication functionality to Boneh&Franklin's Identity-Based encryption scheme
2003	Hess	Efficient Identity Based Signature Schemes Based on Pairings	The paper adds signature and verification functions to Boneh&Franklin's Identity-Based encryption scheme
2003	Boyen	Multipurpose Identity-Based Signcryption: A Swiss Army Knife for Identity-Based Cryptography	The paper combines Identity-Based encryption and signature in one scheme that satisfies all the proposed security requirements, and yet is as compact as pairing-based IBE and IBS in isolation, offers detachable signatures, and supports multirecipient encryption with signature sharing for maximum scalability.
2004	Lee, Boyd, Dawson, Kim, Yang and Yoo	Secure Key Issuing in ID-based Cryptography	The paper proposes a secure key generation scheme in Identity-Based cryptography to keep the privacy of a user's private key and to solve key escrow problem.
2005	Boneh, Boyen and Goh	Hierarchical Identity Based Encryption with Constant Size Ciphertext	The paper proposes an improved hierarchical identity based encryption scheme where the ciphertext size as well as the decryption cost are independent of the hierarchy depth
2007	Chai, Cao and Zhou	Efficient ID-Based Multi-Decrypter Encryption with Short Ciphertexts	The paper proposes an improved Identity-Based multi-decrypter encryption scheme: the number of pairing, multiplication and exoponentiation computation is reduced; the bit length is shortened.

Table II. Summary of Developments of Identity-Based Cryptography

4. IDENTITY-BASED CRYPTOGRAPHY IN MANETS

Since Identity-Based cryptography was proposed and came true in 2001, many researches have been conducted to apply the new technology to MANETs. In the literature, the application covers key management, improvement of PKIs, secure communications, secure routing protocols, and some other topics of MANETs. In the following section, we study the application of Identity-Based cryptography in these areas of MANETs.

4.1 Key Management Using Identity-Based Cryptography

4.1.1 *Preliminaries of Key Management in MANETs.* Key management must solve the problem of sharing a secret among a number of users. Shamir gives a solution to this problem in [Shamir 1979]. In this paper, the author identifies the problem of how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of $k-1$ pieces reveals absolutely no information about D.

The authors proposes a (k, n) threshold scheme to solve this problem based on polynomial interpolation: given k points in the dimensional plane (x_1, y_1) .....(x_k, y_k), with distinct x_i's, there is one and only one polynomial $q(x)$ of degree $k-1$ such that $q(x) = y_i$ for all i. To divide the secret D into n pieces, he suggests picking a random $k-1$ degree polynomial $q(x) = a_0 + a_1x + \cdots + a_{k_i}x^{k-1}$ in which $a_0 = D$, and each piece is the value of the polynomial at the n points: $D_1 = q(1), \cdots D_i = q(i), \cdots, D_n = q(n)$. Thus any subset of k of the pieces can determine the coefficients of the polynomial (using e.g. Lagrange interpolation) and thus the secret data at a certain point. To make this claim more precise, he suggests the use of modular arithmetic instead of real arithmetic. The set of integers modulo a prime number p forms a field in which interpolation is possible.

This scheme was later referred to many times to construct a distributed PKG in Identity-Based cryptography and to solve security problem in ad hoc networks.

Zhou et al suggest the use of Shamir's threshold scheme to secure ad hoc networks in [Zhou and Haas 1999]. This paper was published before the Identity-Based Cryptography was introduced into the area of MANETs , and discussed only how to distribute CA service, but the idea of this paper was later used in many papers using the Identity-Based cryptography, and seems to be the most referenced paper in the ad hoc network security area. We must include this paper if we study security of MANETs. The paper focuses on how to secure routing and how to establish a secure key management service in an ad hoc netwoking enviroment. The authors identify the problem that to establish a key management service using a single CA in ad hoc networks. They suggest distributing this service to an aggregation of nodes.

The authors refer to the work of [Desmedt and Frankel 1989; Desmedt 1994] and indicate that they use the theory of threshold cryptography as a basis for their work. The authors propose a distributed CA architecture and PKI used in ad hoc networks. The CA service, as a whole, has a public/private key pair K/k. The public key K is known to all nodes in the network, whereas the private key k is divided into n shares $s_1, s_2, ..., s_n$, one share for each server. To provide the certificate signing service, "threshold" cryptography algorithm is used – For a

message m, server i can generate a partial signature $PS(m, s_i)$ using its share s_i and forword the signature to a combiner. If $t+1$ out of n partial signature are collected by the combiner, they can jointly perform the operation correctly.

Another contribution made by the authors in this paper is the use of "proactive threshold" scheme to prevent enough share holders being compromised by mobile adversaries. A proactive threshold cryptography scheme uses share refreshing, which enables servers to compute new shares from old ones in collaboration without disclosing the service private key to any server. The new shares constitute a new $(n, t+1)$ sharing of the service private key. After refreshing, servers remove the old shares and use the new ones to generate partial signatures. [2] Share refreshing proceeds as follows [Zhou and Haas 1999, pp 28]:
First, each server randomly generates $(s_{i1}, s_{i2}, \cdots, s_{in})$, an $(n, t+1)$ sharing of 0. Then every subshare s_{ij} is distributed to server j through a secure link. When server j gets the suhshares $s_{1j}, s_{2j} \cdots, s_{nj}$, it can compute a new share s'_j from these subshares and its old share s_j: $s'_j = s_j + \sum_{i=1}^{n} s_{ij}$.

As long as a quorum of servers $(t+1)$ can receive subshares, shares are guaranteed to be refreshed. The scheme works without synchronization requirement.

The authors state that they have implemented a prototype of such a key management service, and the preliminary results have shown its feasibility. But they are unable to give details in their paper due to the space limit.

4.1.2 *Key Generation and Distribution Schemes.* In 2003, about two year after Boneh and Franklin proposed the first fully functional identity-base cryptography scheme [Boneh and Franklin 2001], Khalili et al [Khalili et al. 2003] proposed to use Identity-Based cryptography to secure ad hoc networks. The authors refer to the work of [Zhou and Haas 1999; Bobba et al. 2003] and identify the problem that all proposed key management solutions assume either pre-existing shared secrets between or the presence of a common PKI. They indicate that their paper is an improvement on the method of distributed key management in ad hoc networks.

In this paper, the authors propose to combine efficient techniques from Identity-Based and threshold cryptography to provide a mechanism that enables flexible and efficient key distribution while respecting the constraints of ad-hoc networks. At the time of network formation, the participating nodes form a threshold PKG, and generate - in a distributed fashion – a master public key. The master secret key is shared in a t-out-of-n threshold manner by this initial set of n nodes. All nodes in the network can use their ID as their public key. The secret key, corresponding to the public key, is computed by having the node obtain t shares of their key from a t-out-of-n of the original nodes. All subsequent communications are encrypted and decrypted using the master public key and the ID of the recipient. The authors based their proposal on Boneh's Identity-Based cryptosystem algorithms [Boneh and Franklin 2001].

The authors discuss the selection of identities of nodes and countermeasures against identity spoofing. They suggest the use of Statistically Unique Crypto-

[2]Share refreshing relies on the following homomorphic property. If $(s_1^1, s_2^1, \cdots s_n^1)$ is an $(n, t+1)$ sharing of k_1 and $(s_1^2, s_2^2, \cdots s_n^2)$ is an $(n, t+1)$ sharing of k_2, then $(s_1^1 + s_1^2, s_2^1 + s_2^2, \cdots s_n^1 + s_n^2)$ is a $(n, t+1)$ share of $k_1 + k_2$. If k_2 is 0, we get a new $(n, t+1)$ sharing of k_1.

graphically Verifiable (SUCV) addresses [Montenegro and Castelluccia 2002]. They propose a simpler option to use unpredictable identities. Because identities are unpredictable, an adversary will be unable to obtain someone's personal private key in advance; furthermore, since keys are not reissued the adversary will be unable to obtain a node's personal key once that node has already obtained it. They suggest localizing the spoofing problem in that spoofing only needs to be prevented/detected by the nodes forming the PKG at the time of key issuance (and this can be done by requiring some "unspoofable" supporting material to be presented at the time of a key request); spoofing need not be a concern for other nodes in the network at other times.

The authors state that the main advantage over [Zhou and Haas 1999] is the elimination of requirements to transmit, store, and verify public keys and cerficates. In this paper the authors provide a high-level overview only and refer the reader elsewhere for details.

Deng et al in [Deng et al. 2004; Deng and Agrawal 2004] identify the problem of public key generation and distribution in MANETs. They refer to the work of [Zhou and Haas 1999; J.Kong et al. 2001; Boneh and Franklin 2001] as a basis of their work, and implement an Identity-Based key management and authentication system for MANET. This seems to be the first fully implemented Identity-Based cryptosystem in MANETs.

The authors use Identity-Based and threshold cryptography. The proposed approach consists of two components: distributed key generation and Identity-Based authentication. This paper describes algorithms for master key generation, distributed private key generation, new master key share creation. The system was built on the assumption that each mobile node has a mechanism to discover its one-hop neighborhood and to get the identities of other nodes in the network. The key generation component provides the network master key pair and the public/private key pair to each node in a distribute way. The master key pair is computed collaboratively by the initial network nodes without constructing the master private key at any single node, as Shamir and Zhou suggested [Shamir 1979; Zhou and Haas 1999] [3]. The public key of node ID can be computed as $Q_{ID} = H(ID||Expire - time)$.

When a new node joins a network, it presents its identity, self-generated temporary public key, and some other required physical proof (depending on key issuing policy) to k neighbor nodes and requests PKG service, the master public key and his share of the master private key. Each node in the coalition verifies the validity of the identity of the new node and generates a secret share of a new private key sk encrypted with the temporary public key and sends to the requesting node. By collecting k shares of its new private key, the requesting node would compute its new private key $sk = \sum_{i=1}^{k} s_i Q_{ID}$. It discards its temporary public/private key

[3]Each node C_i randomly chooses a secret x_i and a polynomial $f_i(z)$ over $\mathbb{Z}_q$ of degree $k-1$, such that $f_i(0) = x_i$. Node C_i computes his sub-share for node C_j as $ss_{ij} = f_i(j)$ for $j = 1, 2...n$ and sends s_{ij} securely to C_j. After receiving $n-1$ sub-shares, node C_j can compute its share of master private key as $S_j = \sum_{i=1}^{n} ss_{ij} = \sum_{i=1}^{n} f_i(j)$. Any coalition of k shareholders can jointly recover the secret as in basic secret sharing using $\sum_{i=1}^{k} S_i l_i(z) mod\ q$, where $l_i(z)$ is the Lagrange coefficient. The jointly generated master private key is $SK_M = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} f_i(0)$.

pair, and keeps the new key pair in its memory for the later authentication and communication. Each PKG node also broadcasts the requesting node's network identifier (NID). After this key generation process, the requesting node obtains its new private key sk and all other nodes would register the requesting node into their registration table by entering the node's NID. To initialize the share of master key for the requesting node, each coalition node C_i generates the partial share $s_{ip} = S_i \cdot l_i(p)$ for node C_p ($l_i(p)$ is the Lagrange term). Node C_p obtains its new share by adding the partial shares as $S_p = \sum_{j=1}^{k} s_{p,j}$. The partial shares may be shuffled before being sent to the joining node to protect the secrecy of the coalition nodes' secret shares. The generated keys can provide end-to-end authentication using Identity-Based encryption and signature [Boneh and Franklin 2001].

The authors implemented the scheme into NS-2 and conducted simulations in a network of up to 50 nodes . The authors claim that the most significant advantage lies in the enhancement of security while reducing the communication overhead and resource consumption.

Crescenzo et al in [Crescenzo et al. 2005] introduce Identity-Based threshold signature to MANETs, and propose two new protocols for key generation in MANET using threshold cryptography. They base their work on [Boneh and Franklin 2001], with some modification to it, because they envision that in [Boneh and Franklin 2001] only the message is hashed, then an attack violating the unforgeability property would be possible. In their new scheme they suggest hashing the concatenation of the message and various other parameters; specifically, the threshold parameter, the group size and the indices associated with the parties taking part in this execution of a threshold signature protocol. The partial signature generation S and verification V are as following [Crescenzo et al. 2005, pp 98]:

—S: on input $r \in Z_q$, message $M \in \{0,1\}^*$, threshold t, integer l, client index c and subset $T = \{i_1, ..., i_l\}$ of V, do the following: set $m' = M\|t\|l\|i_1, ..., i_l\|c$,($(V, E)$ denotes the connection graphy over the n parties, the node sends signature request to l parties) , $m = H(m')$ and $\sigma = m_r$; return: $sig = \sigma$.

—V: on input $g, v \in G$, message $M \in \{0,1\}^*$, threshold t, integer l, client index c, subset $T = \{i_1, ..., i_l\}$ of V , and received signature $sig = \sigma$, do the following: compute $m = H(M\|t\|l\|i_1, ..., i_l\|c)$, check that (g, v, m, σ) is a G-DH tuple (whether $c = ab \bmod q$ given $(< G >, g, g^a, g^b, g^c)$). If so, return 1 else return 0. If no signature sig is received then return 0.

In their distributed key generation protocol, each party P_i randomly chooses $a_{i0}, ..., a_{it} \in \mathbb{Z}_q$, defines polynomial $p_i(x) = a_{i0} + a_{i1}x + ... + a_{it}x^t$ (where the operations are performed over $\mathbb{Z}_q$), computes $s_{ij} = p_i(j) \bmod q$ for $j = 1, ..., n$, and computes $A_{ik} = g^{a_{ik}}$ for $k = 0, ..., t$. Each P_i sends A_{ik}, for $k = 0, ..., t$, to all parties and s_{ij} secretly to participant P_j . Then each party P_j verifies the shares received from other parties by checking that, for $i = 1, ..., n$, $g^{s_{ij}} = A_{i0}A_{i1}^{j}A_{i2}^{j^2}...A_{it}^{j^t}$. For any index i for which the check fails, P_j broadcasts a complaint against P_i. If more than t parties complain against P_i, then P_i is disqualified. Otherwise, P_i reveals share s_{ij} for each complaining party P_j.

They prove the partial signature scheme satisfies correctness, unforgeability and robustness (over wired networks) under the assumption that the hash function H

is a random oracle and the group G used is a gap-DH group, while still inheriting the very attractive property of the scheme in [Boneh and Franklin 2001] of having the shortest known signature length. They state that by properly combining the partial signature scheme and the distributed key generation scheme, they can obtain a more efficient threshold signature scheme for MANETs.

Li et al [Li and Han 2005] propose a communication protocol for Id-based key generation in MANET, based on work of [Shamir 1984; Zhou and Haas 1999; Boyen 2003]. The authors point out that share refreshing in [Zhou and Haas 1999] needs a secure channel for delivering subshares, Zhou et al. did not provide the implementation of this secure channel. They propose a signcryption scheme that exactly provides a way for secure transmission, by using periodic private keys, multicast group of PKGs, and key proxy.

They introduce a key proxy for key generation. A key proxy is selected from a group of server nodes: all server nodes form and maintain a few multicast groups according to location. A node floods its RREQ (Routing REQuset) to find a route to the server nodes group. When it receives RREPs (Routing REPly) from server nodes, it selects a server node, say u, which has the shortest path to itself as its key proxy. The routing information to the node u is stored. When it wants to update its private key later, it sends its PREQ (Private key update REQuest) to u and u multicasts the PREQ to all server nodes. The client need not join the group and it only sends a multicast message to the group, which is different from most multicast protocols of ad hoc networks.

The private key of a node is updated periodically: at interval j, a node A computes its public key $D_{A,j} = H(ID_A||j)$, and contacts k server nodes to acquire new private key for time interval $j+1$. Server node computes a partial private key of the client for time interval $j+1$ using its master key share s_i. A's private key $d_{A,j+1} = s_i \cdot D_{A,j}$. Then signcrypts and sends it in a PREP (Private key update REPly) message to A.

In order to check malicious server nodes, at the initial time of the network, PKG publishes a piece of verification information consisting of $g \cdot s_i$ for each server node i. To check the validity of partial key it receives from i, node A needs only to check whether the equation $\hat{e}(D_{A,j+1}, g \cdot s_i) = \hat{e}(d_{A,j+1}, g)$ holds. The PREQ packets are multicast to server nodes group in order to reduce traffic overhead in the network. When it collects PREP packets from k out of n server nodes, the node can reconstruct a new private key using Lagrange interpolation.

They use "proactive threshold" similar to Zhou et al's [Zhou and Haas 1999] [4].

The authors leave the performance analysis of the new scheme as further work.

Zhang et al [Zhang et al. 2005] propose a D-PKG scheme to distribute private key generator (PKG) of Identity-Based cryptography to multiple nodes, based on the work of [Shamir 1984; Zhou and Haas 1999; Boneh and Franklin 2001]. In

[4]Each server node v_s randomly generates $(\sigma_1^s, \sigma_2^s, \cdots, \sigma_n^s)$, an (n,k) sharing of 0. Then it signcrypts $\sigma_l^s, l \neq s$, with its private key and server node v_l's public key. The ciphertext is denoted as c_l. Share refreshing information of server node v_s consists of a vector $(c_1, \cdots, c_{s-1}, 0, c_{s+1}, \cdots, c_n)$. Refreshing information is multicast to the server nodes group. Every server node v_l receiving refreshing information from node v_s can only decrypt ciphertext c_l to recover σ_l^s and learn nothing about other subshare $\sigma_r^s, r \neq l$. When server node v_l gets the subshares $\sigma_l^1, \sigma_l^2, \cdots, \sigma_l^n$, , it can update its share of the system secret key.

D-PKG, the TA supplements the network bootstrapping process with the following operations [Zhang et al. 2005, pp 3517]:

(1) Determine a $(t-1)$-degree $(1 \leq t \leq N)$ polynomial, $h(x) = g + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} (mod\ q)$, with random coefficients $a_i (1 \leq i \leq t-1)$ in $\mathbb{Z}_q$. Here g is the system master-key chosen previously.
(2) Select $n (t \leq n \leq N)$ nodes out of the total N nodes as D-PKGs (distributed private key generators, denoted by SH). Calculate n shares of g as $g_k = h(k)$ for $k \in 1 \cdots n$ and assign g_k to SH_k.
(3) Calculate a set of share commitments as $SC = \{P_k = g_k \cdot P \in \mathbb{G}_1 | 1 \leq k \leq n\}$ ($P \in \mathbb{G}_1$ is an arbitrary generator and a system parameter).

SH and SC are appended to the public system parameters known to every node. Based on the Lagrange interpolation, any combination of t D-PKGs with indices $x_i (1 \leq i \leq t, 1 \leq x_i \leq n)$ in SH can collectively reconstruct the system master-key g by computing $g = \sum_{i=1}^{t} \lambda_i g_x 0$, where $\lambda_i = \prod_{j=1, j \neq i}^{t} \frac{x_j}{x_j - x_i}$.

These D-PKGs collaboratively provide the PKG service: A node B sends them a private-key sub-request containing its public key ID_B. Upon receiving the request, each chosen D-PKG sends back a sub-reply containing a partial private key: $S_{B,x_i} = g_{x_i} H_1(ID_B || otherInfo)$. B can verify its authenticity using P_i: $\hat{e}(S_{B,x_i}, P) = \hat{e}(H_1(ID_B || otherInfo), P_i)$. After obtaining t authentic private-key pieces, B can calculate the complete private key in the same way computing the master-key.

D-PKG also offers anonymity protection to defend against pinpoint attacks using MASK [Zhang et al. 2005], an anonymous on-demand routing protocol designed for MANETs. MASK can fulfill the routing task without disclosing the real identifiers of packet sources and destinations and all the intermediate nodes.

The authors also discuss and determine the optimal secret-sharing parameters (t, n) to achieve the maximum security and designed a novel protocol to dynamically adjust (t, n) to accommodate dynamic node join/leave. They define $Pr_{comp} = \frac{\binom{n}{t}}{\binom{N}{t}}$ as the probability that adversaries happen to pick up and compromise t D-PKGs in one time period so as to reconstruct the system master-key, and $Pr_{para} = \frac{\binom{n}{n-t+1}}{\binom{N}{n-t+1}}$ as the probability that adversaries happen to pick up $(n-t+1)$ D-PKGs and corrupt them in one time period so that there are no enough t D-PKGs to collaboratively provide the PKG service. They further define *Security Level* as $SL_n(t) = 1 - 0.5 Pr_{comp} - 0.5 Pr_{para}$. Based on the definition equation of $SL_n(t)$, they show how the TA can select an appropriate number of nodes as D-PKGs and determine the optimal secret-sharing threshold to achieve the maximum security during the network bootstrapping phase.

This paper presents preliminary results about the application of Identity-Based public-key cryptography in MANETs. As the future research, the authors intend to evaluate and justify the efficacy of the proposed schemes through simulations and practical implementations.

4.1.3 *Key Agreement and Exchange.* Authenticated key exchange among networks nodes in the absence of an online trusted third party is a problem in MANETs. Former solutions based on symmetric keys and PKI requires either the proximity of communicating devices or an online CA.

Hoeper and Gong [Hoeper and Gong 2005a] identify this problem, and propose a set of key exchange protocols using Identity-Based Cryptograhpy scheme, based on the work of [Boneh and Franklin 2001; Hess 2003]. In these protocols, a Trusted Third Party (TTP) computes the private key for each node using a master secret key and node's public key Q_{ID}, and distributes the key over a secure channel during network initialization. After initialiazation, the TTP is not needed, and any two nodes share a pairwise secret key: $K_{AB} = \hat{e}(d_A, Q_B) = \hat{e}(Q_A, d_B) = K_{BA}$. To provide forward security and prevent the TTP from being a key escrow, the authors propose some protocols. A basic form of these protocols is: First, K_{AB} is divided into two parts K_e and K_a. Encryption under K_e prevents all other networks nodes from reading the messages, whereas K_a is used in a message authentication code (MAC) to enable mutual authentication. Then [Hoeper and Gong 2005a, pp 128],

(1) $A \rightarrow B : A, E_{K_e}(K_1)$
(2) $A \leftarrow B : B, E_{K_e}(K_2), MAC_{K_a}(A, E_{K_e}(K_1), E_{K_e}(K_2))$
(3) $A \rightarrow B : MAC_{K_a}(B, E_{k_e}(K_2), E_{k_e}(K_1))$

Shared key can be set up as $K_{ses} = f(K_1, K_2)$.

By replacing K_1 and K_2 with different forms, different properties can be obtained. E.g. using Elliptic Curve Diffie-Hellman protocol, A and B can select ephemeral private keys r_A and r_B, generates and sends public keys $T_A = r_A P$ and $T_B = r_B P$. A shared session can be obtained as $K_{ses} = h(r_A T_B) = h(r_B T_A)$ which is unknown to the TTP and achieves perfect forward secrecy. A revised version of this protocol can be found in their later work [Gong 2007].

The authors analyze what kind of security properties can be achieved by each protocol. They claim the presented protocols resist most of the common attacks, such as impersonation, replay, known-key, unknown-key share and key compromise impersonation. However, they state that these protocols cannot resist active attacks launched by TTP using the system's master key. For future work, they plan to investigate in protocols that provide deniability and resist KCI attacks at the same time.

In [Zhang et al. 2005], Zhang et al point out that most existing group key agreement techniques are not suited to the ad hoc network environment. In literature, Key Predistribution Scheme (KPS) seems to be the best solution for key management in networks whose topology is unknown prior to deployment or changes fast after deployment. The authors arugue that this scheme is not as secure as contributory key agreement. In KPS the group key is selected from a predetermined set; while in contributory key agreement, group key is established through gathering every member's ephemeral secret key. Furthermore, KPS is not suitable for dynamic group, because its session key is determined in advance. Further, the authors state those non-constant round key agreements are not suitable for ad hoc networks, and hence they suggest constant-round contributory key agreement.

Using the IDC scheme of Boneh et al [Boneh and Franklin 2001], the authors revised the constant-round key agreement scheme proposed by Lee et al [Lee and Sriborrirux 2004] that was on password-based. In round 1 of the new scheme, each node generates a ephemeral key $N_i \in \mathbb{Z}_q^*$, computes $z_i = N_i P$, and signs it using the signature scheme of Du et al [Du et al. 2003]: $T_i = H(z_i)sQ_i + N_i P_{pub}$. The node then broadcasts them with its ID:$\langle z_i, T_i, ID_i \rangle$.

In round 2, each of the group member firstly verifies $\hat{e}(\sum_{j\in\{1,\cdots,n\}\setminus\{i\}} T_j, P)$ $= \hat{e}(\sum_{j\in\{1,\cdots,n\}\setminus\{i\}}(H(z_j)Q_j + z_j), P_{pub})$. Then group members are divided into two subgroups and establish two group keys once a time: The member N_i whose index i is odd computes $Y_{iL} = \hat{e}(N_{i-2}P, N_{i-1}P)^{N_i}$, $Y_{iR} = \hat{e}(N_{i+1}P, N_{i+2}P)^{N_i}$, $X_i = H(Y_{iL} \oplus H(Y_{iR}))$. It then signs it using ID-based signature and broadcasts them. The members whose index numbers are even don't broadcast any message for this round information exchange. Each node ID_i in odd index group computes $H(Y_{jL}) = H(Y_{iR}) \oplus X_i \oplus X_{i-2} \oplus \cdots \oplus X_j$ for each odd j. Then this group key can be computed out: $K = H(Y_{1L}) + H(Y_{3L}) + \cdots + H(Y_{nL})$. Similarly do even index members. At last, each node computes a group key that is established through information exchange by even index members K_1 and a group key that is established through information exchange by odd index members K_2.

In summary, for every group key's information exchange at round 2, it only needs about half of group members to take part in, while all members can compute out the same session keys according to the broadcasted messages. This group is divided into two subgroups, and as long as one of these two subgroups doesn't meet with the link failures, this scheme will succeed.

Compared with Du et al's scheme [Du et al. 2003], the authors claim that their scheme avoids the two obstacles for constant-round contributory key agreement in MANET: authenticating the exchanged information without online TTP, and resistance to unstable links.

Chien et al [Chien and Lin 2006] propose an Identity-Based key agreement protocol for MANETs using IBC. The authors begin by referring to the work of Rhee et al [Rhee et al. 2005], Kong et al [Kong et al. 2002] on the problem of key management in MANETs, and indicate that their work is an improvement on the formerly proposed ones.

The authors apply Identity-Based cryptography to the formerly proposed schemes. In their scheme, they divide the whole group into several cell groups and a control group, and each cell group is managed by its cell group controller independently of the other cell groups. Nodes within the same cell group share a cell group key, which can be generated by a distributive or contributory way. The core of their scheme is the *Tripartite key agreement protocol* which allows three parties establish their session keys. The scheme is modified from Hesss signature [Hess 2002] for traditional public key setting. The protocol has two rounds, where the entities broadcast their ephemeral public keys in the first round and the entities broadcast their confirmation (signatures) on the session and ephemeral public keys in the second round [Chien and Lin 2006, pp 524]:

—*1st Round:*
$A \rightarrow B, C : \langle sid, ID_A, ID_B, ID_C, P_A, P'_A\rangle$, Node A computes $P_A = aP, P'_A = a'P$, where a and a' are random numbers chosen by node A, sid is session id.
$B \rightarrow A, C : \langle sid, ID_B, ID_C, ID_A, P_B, P'_B\rangle$
$C \rightarrow A, B : \langle sid, ID_A, ID_B, ID_C, P_C, P'_C\rangle$

—*2nd Round:*
$A \rightarrow B, C : sid, v_A, u_A$
Node A computes $m_A = H_3(sid, ID_A, ID_B, ID_C, P_A, P'_A, P_B, P'_B, P_C, P'_C), r_A = \hat{e}(P, P)^{K_A}, v_A = H_4(m_A, r_A)$ and $u_A = v_A S_A + k_A P$, where K_A is a random

number chose by node A.
$B \rightarrow A, C : sid, v_B, u_B$
$C \rightarrow A, B : sid, v_C, u_C$

A checks whether the following two equations hold: $v_B = H_4(m_B, \hat{e}(u_B, P) \cdot \hat{e}(Q_B, P_{pub})^{-v_B})$ and $v_C = H_4(m_C, \hat{e}(u_C, P) \cdot \hat{e}(Q_C, P_{pub})^{-v_C})$ [5]. Similarly do B and C. After authenticating the message from the other two nodes, A, B, and C share these session keys: $K^1_{A,B,C} = \hat{e}(P_B, P_C)^a, K^2_{A,B,C} = \hat{e}(P_B, P'_C)^a, K^3_{A,B,C} = \hat{e}(P'_B, P_C)^a, K^4_{A,B,C} = \hat{e}(P'_B, P'_C)^a$, $K^5_{A,B,C} = \hat{e}(P_B, P_C)^{a'}$, $K^6_{A,B,C} = \hat{e}(P_B, P'_C)^{a'}$, $K^7_{A,B,C} = \hat{e}(P'_B, P_C)^{a'}$, $K^8_{A,B,C} = \hat{e}(P'_B, P'_C)^{a'}$.

The tripartite key agreement scheme can be easily extended to share n^3 keys by sending n ephemeral public values per node.

The scheme then uses the ternary tree and bilinear map to establish the cell group key. Hierarchical ternary tree is a hierarchical tree, where the degree of a node is at most three. The keys corresponding to the key nodes are generated iteratively from bottom up to the root node, and the key corresponding to the root node is taken as the group key. If a node has three child nodes, then the tripartite key agreement scheme is adopted; otherwise, the two-party key agreement scheme is adopted. In the example shown in Figure 2 , the computation of the first case would be like (K_x denotes Public Key, k_x denotes Private Key): $K_{1,0} = k_{1,0}P, k_{1,0} = \hat{e}(K_{2,0}, K_{2,1})^{k_{2,2}} = \hat{e}(P, P)^{k_{2,0} \cdot k_{2,1} \cdot k_{2,2}}$ The computation of the second case would be like $k_{1,2} = k_{2,6} \cdot K_{2,7} = K_{2,6} \cdot k_{2,7} = k_{2,6} \cdot k_{2,7} \cdot P$. When a node joins or leave the network, or gets compromised, every node updates its group key with the assistance of a sponsor node generating new share and broadcasting update tree.

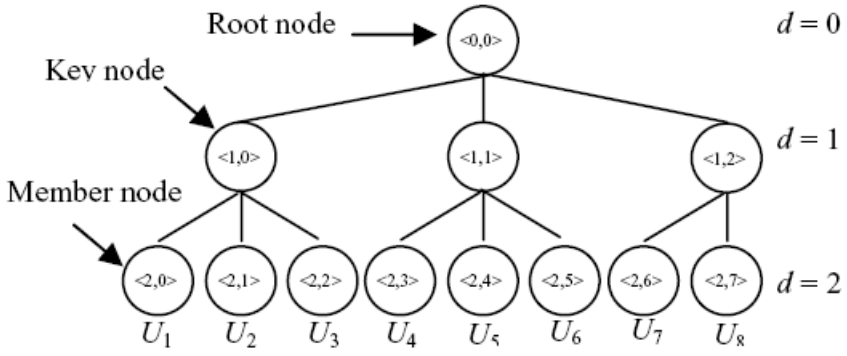

Fig. 2. An Example of a Key Tree ([Chien and Lin 2006, pp 527])

The authors analyze the security and performance of their scheme. They compare it with Hess's scheme [Hess 2002], and claim that it dramatically improves computation and communication efficiency.

[5] $\because \hat{e}(u_B, P) \cdot \hat{e}(Q_B, P_{pub})^{-v_B} = \hat{e}(v_B s Q_B + k_B P, P) \cdot \hat{e}(Q_B, sP)^{-v_B} = \hat{e}(sQ_B, P)^{v_B} \cdot \hat{e}(k_B P, P) \cdot \hat{e}(sQ_B, P)^{-v_B} = \hat{e}(P, P)^{k_B}$

4.1.4 *Key Revocation Schemes.* Due to the weak physical protection of nodes in MANETs, node compromises including key disclosures are very likely. Frequent key renewals to prevent such compromises are either computationally challenging in solution with distributed on-line key generation center (KGC) or infeasible in solutions with off-line KGC. Hoeper et al [Hoeper and Gong 2006b] identify the problem that proposed Identity-Based schemes for MANETs do not provide mechanisms for key revocation and key renewal. They propose a scheme for key revocation and key renewal using an Identity-Based scheme in MANET.

This work is based on their former work in [Hoeper and Gong 2006a], and the work of [Crepeau and Davis 2003; Luo et al. 2002]. To enable key renewal in IBC schemes, they introduce a new format for ID-based public keys: $Q_i = H1(ID_i||t_i||v_i)$, where t_i denotes the expiration date, and v_i is the version number. Note that the version number v always starts with 1 for every new expiry date t and is incremented with each key renewal for the same date t.

In their scheme, each node runs a "neighborhood watch" algorithm to monitor nodes in the communication range for suspicious behavior. These observations are then securely propagated to a m-hop neighborhood.

They discuss and propose a solution for the problems of nodes that wish to revoke their own keys by giving a "*Harakiri*" algorithm in which nodes broadcast $\langle ID_i, d_i, Q_i, (t_i, v_i), \text{"}revoke\text{"}, hopcount\rangle$. Each node maintains an accusation matrix for other nodes. The public key of a node is revoked if at least a threshold – σ nodes accused that node.

New keys can be issued for the same identity after the previous key has been revoked. and new nodes that join the network can learn about past accusations and revocations. Upon receiving a new key pair and re-joining the network, a node only needs to broadcast its new public key to the m-hop neighborhood. The receivers update the version number in their revocation lists accordingly and set all accusation values for this node to zero.

The authors claim their key revocation scheme is scalable in parameters m and σ, i.e. the level of security can be chosen as performance trade-off.

Based on this work, in [Hoeper and Gong 2006a], the authors further present a MANET-IDAKE scheme in which a KGC initializes all devices before they join the network and all tasks are performed by the network nodes themselves without any central KGC. They suggest the of use MAC address as node identity. The lightweight IDAKE protocol provides secure and efficient authentication and key exchange for two network nodes. The schemes only use symmetric cryptography and pairing-based keys which makes them very efficient. Refer to [Hoeper and Gong 2005a] for details.

They claim the protocol is extremely efficient and can be proven secure without perfect forward secrecy in the Canetti-Krawczyk model. They claim to be the first to introduce key revocation and key renewing mechanisms for IBC schemes.

4.1.5 *Avoiding the Key Escrow Problem.* Key escrow is inherent in Identity-Based cryptography. Although it may be a desirable feature in some cases (e.g. in military hierarchy), Hoeper and Gong in [Hoeper and Gong 2005b] and [Hoeper and Gong 2007] identify it as a problem with ad hoc networks. The authors refer to proposed solutions: using additional private/public key pairs [Gentry 2003];

assigning an expiry date to the system's master secret key, or using threshold cryptography to distribute the secret key to multiple nodes [Boneh and Franklin 2001; Lee et al. 2004; Boyd et al. 2004; Chen and Kudla 2003; Oh et al. 2005; Paterson 2002].

The authors propose three adversary models for dishonest TAs, and analyze the probabilities of successful attack for each model. Further, they suggest some countermeasures against this type of attacks: aborting protocols if a node receives messages of different contents that belong to the same protocol flow; two nodes establishing a shared key as soon as they are close to each other; using mobility to enable the use of different routing paths for different protocol flows.

They claim that the special properties of ad hoc networks combined with the presented countermeasures prevent a TA from being a key escrow in most ad hoc network applications. For future work, they plan to further investigate their third adversary model and explore more applications of that model.

In another of their papers [Hoeper and Gong 2007], they explain this idea in more detail: the authors identify the key escrow problem of dishonest PKG or a colluding group of PKGs, and the problem of utilizing key escrow.

They derive two adversary models for dishonest PKGs in MANETs, analyze the attack probabilities and propose contermeasures. For model 1 – Dishonest PKG model, they conclude that passive attacks by dishonest PKGs can be easily prevented by implementing a Diffie-Hellman (DH)-like key agreement protocol or any other protocol that provides Perfect Forward Secrecy. They propose a protocol for this use: A and B generate an ephemeral keys $T_A = r_A P$ and $T_B = r_B P$, where r_A and r_B are random nonces and P a generator of the elliptic curve. Then session key $K = r_A T_B = r_B T_A$, and A and B obtain session key in this way [Hoeper and Gong 2007, pp 4]:

(1) $A \longrightarrow B$: A, s, T_A (s is a session identifier)
(2) $B \longrightarrow A$: $B, s, T_B, f_{K_{AB}}(A, T_A, s, T_B)$ ($f()$ is a pseudorandom function)
(3) $A \longrightarrow B$: $A, s, f_{K_{AB}}(B, T_B, s, T_A)$

Even though they believe that an active attack is very unlikely in Model 1, they introduce some contermeasures to decrease the probability [Hoeper and Gong 2007, pp 8]:

—Session control. Network nodes acting as a router discard all received messages that belong to the same protocol flow but have different contents. This can be detected by checking the session identifier and the message format in packets.
—Close proximity. Two nodes should establish a new shared key as soon as the nodes are in close proximity to each other because close proximity of nodes makes successful attacks very unlikely.
—Disjoint Paths. Using different routing paths for packets whenever possible.
—Distributed PKGs. Using (k, n)-threshold or other schemes to distribute the power of PKGs.

For model 2 – Spy nodes model, they use same contermeasures for passive attacks. For active attacks, they suggest the following countermeasures [Hoeper and Gong 2007, pp 9]:

—One-hop communications. Two nodes establish a fresh shared key whenever they are in direct communication range.

—Close proximity. Two nodes should derive a session key whenever the distance between them is small.

—Delay detection. If a flow takes more time than an estimated delay, the session is dropped.

—Distributed PKGs. Using (k, n)-threshold or other schemes.

The authors also studied the problem of utilizing key escrow. They conclude that increasing the number of deployed spy nodes, giving them more communication power and placing them at strategic places, can significantly improve the ability of a PKG to act as key escrow.

As future work, the authors will simulate their models and investigate different routing protocols.

4.2 IBC Based PKIs for MANETs

Traditional Public Key Infrastructure (PKI) is based on Public Key Certificate (PKC). In MANETs, because the computational and communication resources required by PKC operations are very limited, and also a centralized CA is not reliable, traditional PKI is regarded unsuitable [Lin et al. 2005]. By applying Identity-Based cryptography to MANETs, new hybrid PKIs combining traditional PKIs with IBC technologies can be setup and adapted to MANETs.

In [Lin et al. 2005], the authors identify the difficulty of appling traditional PKI security architecture to MANET. They suggest the use of a hybrid architecture that combines the good sides of both traditional PKI and Identity-Based schemes, and propose a novel scalable and robust cluster-organized key management scheme.

Based on former work of [Boneh and Franklin 2001; Huang and Lin 2003; Zhou and Haas 1999; Shamir 1984], they propose a novel cluster-organized key management scheme and integrate it into secure routing protocols. The proposed network framework is a two-layer hierarchical structure performing key generation, key distribution, and storage. The bottom layer is responsible for internal cluster domain authentication using Identity-Based scheme, and the upper layer, root CA, is responsible for external cluster domain authentication. The advantage of two-layer key management scheme is to distribute the central key management functionality to a number of CAs.

An Identity-Based scheme is introduced in every cluster domain. Cluster heads can only maintain identities of members, without needs to store and distribute public keys. The cluster head serves as the PKG for cluster members. When a node joins the network, it is given a master-public-key belonging to a cluster domain. Furthermore, each node also applies for a personal private-key from its cluster domain head, and uses it to achieve routing packets and messages encrypted/decrypted capability. The Identity-Based key generation and distribution use Boneh's algorithms.

The authors implemented the scheme and simulated it with NS-2. They conducted simulations under mobility model and traffic model to simulate the updated convergence time of sharing keys, the packet delivery ratio, and routing overheads.

They state the simulation results demonstrate that the scheme can reduce computing loads of central CA and key repositories.

Saxena [Saxena 2006] proposes a scheme of PKI for MANET analogous to Identity-Based cryptography with some claimed advantages. His work is based on the work of [Zhou and Haas 1999; Shamir 1979; Feldman 1987] on threshold cryptography and work of [Boneh and Franklin 2001] on Identity-Based cryptography.

He suggests the use of Feldman's *Verifiable Secret Sharing (VSS)* to generate private keys and public keys. In order to setup the system, a dealer (or a set of co-founding members) first chooses appropriate parameters (p, q, g) for the group, and selects a polynomial $f(z) = a_0 + a_1 z + \cdots + a_t z^t$ in Z_q, where a_0 is the group secret. The dealer keeps the polynomial secret and publishes commitments to the coefficients of the polynomial, as $w_i = g^{a_i}(mod\ p)$, for $i = 0, \cdots, t$. To join the group, a user M_i sends its unique identifier id_i to the dealer who issues it its secret share $x_i = f(id_i)(mod\ q)$ [6]. The public key $y_i = g_i^x(mod\ p)$ of M_i can be computed as $y_i = \prod_{j=0}^{t}(w_j)^{id_i^j}(mod\ p)$. Also M_i can compute M_j's public key as: $y_j = \prod_{i=0}^{t}(w_i)^{id_j^i}(mod\ p)$, and pairwise shared key as: $k_{ij} = y_j^{x_i} = g^{x_j x_i}(mod\ p)$. With these keys, they define the sign/verify and encrypt/decrypt as [Saxena 2006, pp 382]:

—*Sign*: To sign a message m, M_i (having secret key x_i), picks a random secret $k \in Z_q$ and computes $r = g^k(mod\ p)$. It then outputs the signature as a pair (c, s), where $c = H(m, r)$ and $s = k + rx_i(mod\ q)$.

—*Verification*: In order to verify the above signature (c, s), a recipient first computes the public key y_i of the signer M_i using its identity id_i as $y_i = \prod_{j=0}^{t}(w_j)^{id_i^j}$ $(mod\ p)$, and then verifies whether $c = H(m, r)$, where $r = g^s {y_i}^{-c}(mod\ p)$.

—*Encryption*: In order to encrypt a message m for a user M_i in the group, the encryptor computes the public key of M_i as $y_i = \prod_{j=0}^{t}(w_j)^{id_i^j}(mod\ p)$, chooses a random $r \in Z_q$ and then sends a pair (c_1, c_2) to M_i, where $c_1 = g^r(mod\ p)$ and $c_2 = m \oplus H(y_i^r)$.

—*Decryption*: M_i recovers the message by computing $c_2 \oplus H({c_1}^{x_i})$ from the ciphertext (c_1, c_2).

The authors point out that their proposed scheme can be viewed as an Identity-Based cryptosystem based on threshold assumption. Knowing the identifier of a particular user and also the public key of the trusted center, one can send encrypted messages and verify signatures. This is equivalent to IBE and ID-based signatures. They further state that unlike other ID-based schemes, their proposal is based on standard (discrete logarithm) assumptions; moreover, for reasonable group sizes and threshold values, their scheme is much more efficient than these prior ID-based schemes, which require costly computations (such as scalar point multiplications, map-to-point operations and bilinear mappings in [Boneh et al 2001]) in elliptic-curves.

[6]The secret share x_i can be validated as in [Crescenzo et al. 2005]

4.3 Secure Communications Using Identity-Based Cryptography

Some researchers propose the use of Identity-Based cryptography for secure communication in MANETs, which includes: anonymous communications, pairwise communications, and broadcasting etc.

Zhang et al apply IBC to anonymous communications in MANETs [Zhang et al. 2005]. The authors identify the problem of malicious traffic analysis in MANETs, due to the broadcast nature of radio transmission. Derived from pairing-based cryptography [Boneh and Franklin 2001; Balfanz et al. 2002], the authors propose an anonymous neighborhood authentication protocol which allows neighboring nodes to authenticate each other without revealing their identities, and a key management scheme on per link basis which facilates an anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks.

The PKG pre-calculates a large set of collision-resistant pseudonyms and a corresponding secret point set. During the bootstrapping phase, a trusted authority (TA), e.g. the system administrator or network planner (not entering the network), distributes system public parameters as Boneh suggested [Boneh and Franklin 2001]. Moreover, the TA furnishes each node ID_i with a sufficiently large set PS_i of collision-resistant pseudonyms and a corresponding secret point set as $S_i = \{gH_1(PS_{i,j}) \in \mathbb{G}_1\}(1 \leq j \leq |PS_i|)$. No one but the PKG can link a given pseudonyms to a particular node or identity, or deduce the corresponding secret point with non-negligible probability. The anonymous neighborhood authentication protocol works like this [Zhang et al. 2005, pp 1943]:

(1) $A \rightarrow B : \langle PS_A, n_1 \rangle$

(2) $A \leftarrow B : \langle PS_B, n_2, V_0 \rangle$, where $V_0 = H_2(K_{BA}||n_1||n_2||0)$,
$K_{BA} = \hat{e}(sH_1(PS_B), H_1(PS_A))$

(3) A computes $V_0' = H_2(K_{AB}||n_1||n_2||0)$, where $K_{AB} = \hat{e}(H_1(PS_B), sH_1(PS_A))$
and check if $V_0 = V_0'$, then
$A \rightarrow B : \langle V1 = H_2(H_2(K_{AB}||n_1||n_2||1) \rangle$

(4) B computes $V_1' = H_2(K_{BA}||n_1||n_2||1)$, and check if $V_1 = V_1'$

Note that A and B actually broadcast the above messages in a neighborhood.

After a successful handshake, both A and B can calculate γ pairs of shared session key ($SKey$) and link identifier ($LinkID$) as: $K_{AB}^{\gamma} = H_2(K_{AB}||n1||n2||2*\gamma)$, $L_{AB}^{\gamma} = H_2(K_{AB}||n1||n2||2*\gamma+1)$. Such $\langle SKey, LinkID \rangle$ pairs are unique due to collision-resistant hash functions H_1 and H_2. The $LinkID$s will be used to identify the packets transmitted between A and B and the $SKey$ can be used to encrypt, integrity-protect, or authenticate the content of the packets if needed.

Based on this anonymous neighborhood authentication scheme, the authors propose an improved AODV routing protocol which enable communication between nodes without disclosing the real identity of the node.

The authors evaluated the computation costs of the critical cryptographic operations in their scheme: SHA-1 and RC6 were evaluated using the Crypto++ Library S.1 and the Tate pairing was evaluated within the MIRACL Library. In their current implementation, the routing information is not authenticated, they plan to

combine MASK with other secure routing schemes to provide an anonymous yet secure routing protocol.

Bohio et al apply IBC to secure group communications and broadcasting. In [Bohio and Miri 2004b], the authors propose a non-probabilistic method for computing unique broadcast keys for different groups. Based on work of [Cha and Cheon 2003], they use Identity-Based pairwise symmetric keys as the building block for their broadcast scheme. They state such keys are computed non-interactively by the nodes, which reduces communication overhead and simplifies key management in pairwise communication.

The group key is generated in this way: Let K_{1N} be the broadcast secret of node 1 for any group of N nodes. Node 1 computes its broadcast parameter $P_{1-brdcst}$ as: $P_{1-brdcst} = K_{1N} \cdot Q_{id_1}$, and distributes it to all candidate nodes using respective pairwise encryption. To sign and encrypt a message M, node 1 computes:
$h = H_3(M)$, where $H_3 : \{0,1\}^* \rightarrow \{0,1\}^*$;
$K_{1-brdcst} = H_2(\hat{e}(Q_{id_1}, P)^{(r+h)})$, where $r \in Z_q^*, H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^m$;
$C = M \oplus K_{1-brdcst}$, $U = rP$, $V = K_{1N}^{-1}(r+h)P$.
The broadcast message is: $\langle C, U, V \rangle$. Every node in the group can compute the same broadcast key $K_{1-brdcst}$ as node 1 from $H_2((P_{1-brdcst}, V))$ and decrypt the message from the cipher text C as: $M = C \oplus K_{1-brdcst}$; After decrypting message , its hash can be computed as: $h = H_3(M)$, and authentication is verified by checking if $\hat{e}(K_{1N}Q_{id_1}, V) = \hat{e}(Q_{id_1}, U + hP)$ holds.

Also in the paper, the authors suggest one use of this broadcasting scheme for threshold cryptography: a secure and efficient channel for broadcasting secret shares among the PKG servers. They authors envision the shortcoming of the scheme proposed in [Khalili et al. 2003] where each server node encrypts and signs each message separately. With their suggested scheme, the group key is establised in the first round, and then all the messages can be encrypted and signed using this group key.

In [Bohio and Miri 2004a], the same authors indicate that the use of pairwise communication creates additional bandwidth overhead in case of broadcast messages. They propose an authenticated broadcast scheme based on symmetric keys and a corresponding signature scheme. Based on work of [Boneh and Franklin 2001] and their former work [Bohio and Miri 2004b], the authors extend pairwise shared key generation method proposed in [Sakai et al. 2000] – $K_{AB} = K_{BA} = \hat{e}(Qid_A, sQid_B)$, and propose a method for computing collisionfree broadcast keys that can be used for different groups in the network and changed as the group membership varies. Such keys can be useful in the context when it is important to have all the broadcast keys unique without causing additional handshake between the nodes.

Compared to [Bohio and Miri 2004b], the authors simplify the scheme as: Node 1 computes its broadcast parameter $P_{1-brdcst}$ as: $P_{1-brdcst} = K_{1N} \cdot P$, and distribute it to all candidate nodes using respective pairwise encryption. Every node will then compute the broadcast key of node 1 as $K_{1-brdcst}$ using the hash function $H_3 : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow (0,1)^m$ which outputs a key of size m for the input of two elements of group $\mathbb{G}_1$. The key $K_{1-brdcst}$ is: $K_{1-brdcst} = H_3(P_{1-brdcst})$. To generate unique broadcast secret K_{1N} for node 1, let $D_{1N} = \hat{e}(sQ_{id_1}, Q_{id_2} + Q_{id_3} + \cdots + Q_{id_n}) = \hat{e}((sQ_{id_1}, Q_{id_2}) \cdot$

$\hat{e}((sQ_{id_1}, Q_{id_3}) \cdots \hat{e}((sQ_{id_1}, Q_{id_n})$ and $K_{1N} = H_2(D_{1N})$. Further, the authors use this group key to sign group messages M: $\langle U, V\rangle = \langle rQid_1, K_1N^{-1}(r+h)Qid_1\rangle$ where $r \in Z_q^*$, $h = H_4(M)$. And the receiver can verify if $\hat{e}(P_{1-brdcst}, V) = \hat{e}(P, U + hQ_{id_1})$ holds.

The authors claim that the advantage of the group broadcast key is that it needs only n private keys to be generated and distributed to n nodes by TA, whereas previous schemes need $n(n-1)/2$ and $n(n-1)$ respectively. The use of signatures in broadcast messages saves bandwidth being used in comparison to the case when broadcast messages are sent using pairwise encryption for each node separately.

The authors point out one potential problem of this scheme is that it might be possible for malicious nodes to generate computational overhead for other nodes by sending unnecessary broadcast messages. The countermeasure is the non-repudiation and authentication provided by the signature in the scheme.

In [Bohio and Miri 2004c] – the extended version of [Bohio and Miri 2004b] and [Bohio and Miri 2004a] – the authors reiterate their scheme to generate collision-free broadcast keys for different groups and an authenticated broadcast scheme based on symmetric keys and a corresponding signature scheme. On the basis of the former two papers, the authors present two varieties of their former scheme to work around key escrow problem:

The first scheme is based on group identity. A group public key Q_{GRP-ID} is to be generated by the TA based on any group identity or arbitrary string. The TA, using its master keys, then computes the initial group key $D = s \cdot Q_{GRP-ID}$. Every node i will then receive the point D from the TA and will generate its private key k_i, a random secret, and compute the corresponding public key as $D_{i-pub} = k_i \cdot D$. All such individual public keys should be available from the TA. The participating nodes then get the public key of every node from the TA.

Any node 1 using its private key k_1 and the public key of node 2, i.e. k_2D, can compute k_1k_2D, and similarly node 2 will use its private key k_2 and public key of node 1 and will compute k_2k_1D. Node 1 and 2 will then compute: $K_{12} = H_3(k_1k_2D)$. Each pair of nodes can compute their pairwise secret key in this way.

For the broadcast key, the parameter $P_{1-brdcst} = K_{1N} \cdot P$ is computed as in the basic scheme with K_{1N} being any random secret. The signature scheme would be used as in the basic model.

The second scheme is based on individual identity. The TA will compute the partial private key of any node i as $D_i = s \cdot Q_{id-i}$. Node i computes its private key as $k_i = H_3(x_i \cdot D_i)$, where x_i is a random secret chosen by node i. It computes public key as $D_{i-pub} = k_i \cdot P$, and submits it to the TA. The pairwise and broadcast keys will be computed similarly as the first scheme does.

They state the advantage of their broadcasting scheme is that the scheme does not use certificates and removes the key escrow inherent in the conventional Identity-Based cryptosystem.

4.4 Secure Routing Protocols Using Identity-Based Cryptography

Another important use of Identity-Based cryptography in MANETs is to design secure routing protocols. Lee, Kim, Chung and Yoon in [Lee et al. 2003] identify the requirement of a secure routing protocol in MANET. They then review some proposed solutions: Ariadne, ARAN (Authenticated Routing for Ad hoc Networks),

and SRP (Secure Routing Protocol), and analyze their weaknesses. They suggest the use of Identity-Based cryptography [Boneh and Franklin 2001; Paterson 2002] in a secure routing protocol.

In their routing protocol, the form of a route request packet is $\langle RReq, SourceID, DestinationID, seq, Sign_S(M), (IntermediateIDList), W, U, V\rangle$, where $M = \langle RReq||SourceID||DestinationID||seq||W\rangle$.

Assume $Q_i = n_i \cdot P$. The source node signs the packet as follows:
Generates a random string $\sigma_S \in \{0,1\}^n$, computes $r = H_3(ID_{Source}, \sigma_S)$;
Using r and its private key sn_sP computes: $\hat{e}(rP, sn_SP) = g^{rsn_S}, (g = \hat{e}(P,P))$, $(\hat{e}(sP, Q_{Dest}))^r \oplus r = (\hat{e}(sP, n_DP))^r \oplus r = g^{rsn_D} \oplus r$. A final RReq packet is like: $\langle RReq, ID_Source, ID_Dest, seq, Sign_S(M), (IntermediateIDList), rP, g^{rsn_S} \times \sigma_S, g^{rsn_D} \oplus r\rangle$.

An intermediates node i that receives route request packet verifies the signature value. If it is correct, adds ID_i to the $intermediateIDList$, computes the new value of U by: $U = U \times \hat{e}(rP, sn_iP)$, and then rebroadcast the packets generated.

A destination node D that received routing request packet and whose ID is matched to value of $DesrinationID$ field in the packet performs the following procedure: computes r' using private key of D and the values of packet received: $r' = V \oplus \hat{e}(W, sn_DP)$, gets the public keys of the ID'S that are described in $intermediateIDList$ and computes $A = [\hat{e}(sP, \sum_{i=1}^{k} n_iP)]^r$. Using A value, D computes $\sigma' = U \times A^{-1}$ [7], and compares r' and $H_3(\sigma', ID_S)$. If the two values are equal, D makess route reply packet as $\langle RRep, seq, (ID_S, ID_1, ..., ID_k, ID_D), W, V \oplus \sigma', Sign_D(M)\rangle$, where $M = \langle RRep||seq||ID_S||ID_1||...||ID_k||ID_D||W||V \oplus \sigma'\rangle$

After receiving the route reply packet, the intermediate nodes in routing path and source node S verify the signature of D. And if it is correct, they add the path in the packet to their route cache.

The authors then analyze the security of their protocol. They compare its performance with the afore-mentioned secure routing protocols, and conclude that their protocol is more efficient than them. They point out a weakness of their new protocol: An attacker can do resource consumption attacks using valid packets of passing the verification procedure. They suggest that an attack can be prevented by using other network features such as counting number of packets per some duration and additional policy.

Park, Myung and Lee in [Park et al. 2005] identify the problem that former routing protocols neglect the inheritance features of ad-hoc network such as limited resources and computational ability. They suggest the application of Identity-Based cryptography to improve these protocols. They base their work on [Boneh and Franklin 2001; jacques Quisquater 2003].

Their protocol is similar to [Lee et al. 2003], but the signature and verification procedures are different:
When source sends $RReq$ to intermediate, the packet format is: $\langle RReq||ID_S||(r_S, Z_S)||$ $Sign_S(H(M))\rangle$, where $M = \langle RReq||ID_S||(r_S, Z_S)\rangle$, $r_S = H(\hat{e}(P,sP)^x||P_{pub-S}||RReq)$, $Z_S = xsP - rsQ_S$, x is a random number.

An intermediate node X_i computes $k' = \hat{e}(P, Z_S) \cdot \hat{e}(P, sQ_S)^r = \hat{e}(P, xsP)\hat{e}(P, -rsQ_S)\hat{e}(P, rsQ_S) = \hat{e}(P,P)^{xs}$ for the authentication of the node which sends the

[7] It is an error to use V instead of A in the published paper

message, and it checks $r_S = H(k'||P_{pub-S}||RReq)$. If the verification is successful, the intermediate node can trust the received message and then it computes r_X and Z_S similarly, and broadcasts the message to the next node as:
$\langle RReq||ID_S||ID_X||(r_S, Z_S)||(r_X, Z_X)||Sign_S(H(M))\rangle$.

When the destination node receives this message, it checks the destination address. If the destination address is the same as its address, it verifies the signature, (r_S, Z_S) and (r_X, Z_X). If the verification process is successful, it is ready to reply a message. The destination node sends a $RREP$ message to the source node. After passing intermediate nodes the reply message is like:
$\langle RRep||ID_D||ID_X||(r_D, Z_D)||(r_X, Z_X)||Sign_S(H(M'))\rangle$.

The authors conducted empirical studies using NS-2 to evaluate the effectiveness of LSRP, and claim that the simulation results show that the LSRP is more efficient in terms of cost and overhead than RSA-based protocols.

Park and W. Lee in [Park and Lee 2005], Park and Myung and W. Lee in [Park et al. 2004], W. Lee and Sriborrirux in [Lee and Sriborrirux 2004] present the same work independently.

Song et al in [Song et al. 2005] apply Identity-Based multi-signature to routing protocols in MANETs. They identify the problem of multi-signature in MANETs. The traditional way to do this is to have each node sign each message, and the resulting signature is large. The authors propose a sound authentication mechanism with aggregation signature, based on the work of [Boneh et al. 2003; Cha and Cheon 2003].

In their scheme, an aggregate signature can be generated on distinct messages: assume $\sigma = (U, V)$ is the signature on messages $M_1, \cdots, M_{i-1}$, and $\sigma = (U', V')$ is the signature on messages M_i, $U = rQ_{ID}, h = H_1(M_1, ...), V = (r + h)d_{ID}$. The aggregator verifies that M_i is different from any other messages. If it is true, it computes: $U = U + U' \in \mathbb{G}_1, V = V + V' \in \mathbb{G}_1$. Then $\sigma = (U, V)$ becomes the aggregate signature on $M_1, \cdots, M_i$. The destination can verify the validity of the aggregation signature: Given identities $ID_1, ..., ID_n$, distinct messages $M_1, ..., M_n$, and an aggregate signature $\sigma = (U, V)$, the verifier computes $h_i = H_1(M_i)$ for all $1 \leq i \leq n$. Then it checks whether $\hat{e}(\sum_{i=1}^{n} h_i Q_{ID_i} + U, P_{pub}) = \hat{e}(\sum_{i=1}^{n} [(h_i + r_i)Q_{ID_i}], P_{pub}) = \hat{e}(\sum_{i=1}^{n} [(h_i + r_i)d_{ID_i}], P) = \hat{e}(V, P)$ holds. If it is true, all the signatures are valid.

They then demostrate in the paper the use of this scheme in on-demand routing protocols such as DSR and AODV: A route request message contains six fields: $\langle RREQ, initiator, target, seq, nodelist, aggsign\rangle$. where the *nodelist* is a list of intermediate nodes on the route between *initiator* and *target* nodes, and the *aggsign* is a aggregate signature integrated by initiator and intermediate nodes. An intermediate node adds its identity to the *nodelist* and generates its own signature on the following fields: $\langle RREQ, initiator, target, seq, nodelist\rangle$, and aggregates its signature into the aggregate signature *aggsign*, then re-broadcasts the message. The length of aggregate signature, does not change, so it does not require any communication overhead. A route reply message contains the following fields: $\langle RREP, target, initiator.seq, nodelist, sign\rangle$. The $target, initiator, nodelist$ fields are set to the corresponding values from the RREQ message. The *seq* is incremented whenever the target node issues a new RREP and the *sign* is a signature of the target node.

The authors compare this scheme with RSA based signature scheme, and state their scheme is more efficient with less length.

Adjih et al [Adjih et al. 2005] identify the problem of secure routing using OLSR in MANETs. They present the attack tree towards OLSR protocol, and analyze the possible attacks. They propose a security architecture to secure OLSR.

Their proposal is based on the work of [Cha and Cheon 2003; Boneh et al. 2001]. In their scheme, an (offline) Trusted Authority is in charge of certifying or assigning keys of each node participating in the trusted network. Each node joining the network will have the public key of of the TA. This key is denoted the global key. Later, any node entering the ad-hoc network could diffuse its public keys, with a specific key exchange protocol, with proper parameters and signatures. The key which is used later to sign message is called the local key, and can be either its global key, or newly generated private/public keys. A node would start originating OLSR control messages, signing them using the local key with a specific extension which prepends a special signature message.

The authors analyze their scheme against possible attacks, compare the performance of Identity-Based cryptography and traditional symmetric cryptography, and claim that Identity-Based cryptography signaficantly improves the performance. At the time the paper, they were at designing stage of their system, thus they only presented their rough idea without giving implementation details.

4.5 Peer Collaboration in MANETs using Identity-Based Cryptography

Cai et al [Cai et al. 2005] apply Identity-Based cryptography to peer collaboration in MANETs. They identify the problem of peer collaboration in ad hoc networks, especially when some peers are autonomous, selfish, or malicious in large-scale, heterogeneous networks. Payment-incited mechanism is an approach for this problem, but most existing electronic payment schemes either rely on online, interactive authorities, or are too heavy (in terms of computation and communication complexity) for wireless ad hoc networks. The authors design a lightweight and cheat-resistant micropayment scheme to stimulate and compensate collaborative peers that sacrifice their resources to relay packets for other peers. They base their work on the latest advances in Identity-Based cryptography at that time [Gentry and Silverberg 2002; Boneh and Franklin 2001]. Their scheme uses Identity-Based signature and verification mechanisms to achieve authentication and non-repudiation of commitment proposal messages and commitment confirmation messages, and uses hash-chain to count data volume transmitted.

The authors conducted simulations of their schemes. Through simulation results, they claim that when security and collaboration measures are properly enforced, profitable collaboration is a preferable strategy for all peers in wireless ad hoc networks; and with profitable collaboration, system utility increases when peers have maximized their potential profit.

4.6 Summary

In this section, we have studied application of Identity-Based cryptography in MANETs in the areas of: key management, improvement of PKIs, secure communications, secure routing protocols, and peer collaboration of MANETs. In Tables III, IV, V, we summarize these proposals and the corresponding papers.

Year	Author(s)	Title of Paper	Main Contribution(s)	Area
1979	Shamir	How to Share a Secret	The paper proposes a threhold scheme to share secret among several parties.	Key Management
1999	Zhou and Haas	Securing Ad Hoc Networks	The paper suggests the use of threshold cryptography to secure ad hoc networks, answers how to establish a secure key management service in an ad hoc netwoking enviroment, and proposes "proactive threshold" scheme to prevent enough share holders being compromised by mobile adversaries.	Key Management
2003	Khalili, Katz and Arbaugh	Toward Secure Key Distribution in Truly Ad-Hoc Networks	The paper suggests the use IBC of to secure ad hoc networks, and proposes a high-level overview to implement their idea.	Key Management
2003	Lee, Kim, Chung, Lee and Yoon	On-demand secure routing protocol for ad hoc network using ID based cryptosystem	The paper applies IBC to a secure routing protocol, and uses IBC signature to sign and verify Routing Request and Routing Reply packets.	Secure Routing
2004	Deng and Agrawal	"Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks" and "TIDS: threshold and Identity-Based security scheme for wireless ad hoc networks"	The paper seems to be the first implementation of a key management and authentication system for MANETs using Identity-Based and threshold cryptography.	Key Management
2004	Crescenzo, Arce and Ge	Threshold Cryptography in Mobile Ad Hoc Networks	The paper introduces Identity-Based threshold signature to MANETs, and proposes two new protocols for key generation in MANETs using threshold cryptography.	Key Management
2004	Bohio and Miri	An Authenticated Broadcasting Scheme for Wireless Ad Hoc Network	The paper applies IBC to secure group communications and broadcasting, and proposes a non-probabilistic method for computing unique broadcast keys for different groups.	Secure Communication
2004	Bohio and Miri	Authenticated secure communications in mobile ad hoc networks	The paper proposes an authenticated broadcast scheme based on symmetric keys and a corresponding signature scheme.	Secure Communication
2004	Bohio and Miri	Efficient Identity-Based security schemes for ad hoc network routing protocols	The paper proposes a scheme to generate broadcast keys for different groups and an authenticated broadcast scheme based on symmetric keys and a corresponding signature scheme, and presents two varieties of their former scheme to work around key escrow problem.	Secure Communication

Table III. Summary of Applications of Identity-Based Cryptography in MANETs

2004	Park, Myung and Lee	ISSRP: A Secure Routing Protocol Using Identity-Based Signcryption Scheme in Ad-Hoc Networks	The paper proposes a routing protocol similar to [Lee et al. 2003].	Secure Routing
2004	Lee and Sriborrirux	Optimizing Authentication Mechanisms Using ID-Based Cryptography in Ad Hoc Wireless Mobile Networks	The paper presents the same work as in [Park et al. 2005].	Secure Routing
2005	Li and Han	A New Scheme for Key Management in Ad Hoc Networks	The paper proposes a communication protocol for Identity-Based key generation in MANETs, a signcryption scheme that provides a way for secure transmission for threshold cryptography; The paper proposes periodic private keys, multicast group of PKGs, and key proxy.	Key Management
2005	Zhang, Liu, Lou, Fang, and Kwon	AC-PKI: anonymous and certificateless public-key infrastructure for mobile ad hoc networks	The paper proposes a D-PKG scheme to distribute PKG of Identity-Based cryptography to multiple nodes. The paper discusses and determines the optimal secret-sharing parameters to achieve the maximum security and designed a novel protocol to dynamically adjust them to accommodate dynamic node join/leave.	Key Management
2005	Hoeper and Gong	Identity-Based Key Exchange Protocols for Ad Hoc Networks	The paper proposes a set of key exchange protocols using identity based cryptograhpy scheme.	Key Management
2005	Zhang,Ye, Li, Cheng and Ma	Constant-round contributory group key agreement for ad hoc networks	The paper suggests contributory key agreement be more secure for MANETs, and proposes a constant-round contributory key agreement scheme.	Key Management
2005	Hoeper and Gong	Limitations of Key Escrow in Identity-Based Schemes in Ad Hoc Networks	The paper proposes three adversary models for dishonest TAs, and analyzes the probabilities of successful attack for each model.	Key Management
2005	Lin, Huang and Wang	Resilient Cluster-Organizing Key Management and Secure Routing Protocol for Mobile Ad Hoc Networks	The paper suggests the use of a hybrid architecture that combines the good sides of both traditional PKI and Identity-Based schemes, and proposes a novel scalable and robust cluster-organized key management scheme.	PKI
2005	Zhang, Liu and Lou	Anonymous communications in mobile ad hoc networks	The paper proposes an anonymous neighborhood authentication protocol which allows neighboring nodes to authenticate each other without revealing their identities, and a key management scheme on per link basis which facilates an anonymous on-demand routing protocol to enable anonymous communications thereby thwarting possible traffic analysis attacks.	Secure Communications

Table IV. Summary of Applications of Identity-Based Cryptography in MANETs (cont'd I)

2005	Park, Myung and Lee	LSRP: A Lightweight Secure Routing Protocol with Low Cost for Ad-Hoc Networks	The paper proposes a routing protocol similar to [Lee et al. 2003], but the signature and verification procedures are different.	Secure Routing
2005	Park and Lee	ISMANET: A Secure Routing Protocol Using Identity-Based Signcryption Scheme for Mobile Ad-Hoc Networks	The paper proposes a routing protocol similar to [Lee et al. 2003].	Secure Routing
2005	Song, Kim, Lee and Yoon	Security enhancement in ad hoc network with ID-based cryptosystem	The paper applies Identity-Based multi-signature to routing protocols in MANETs, and proposes a sound authentication mechanism with aggregation signature to authenticate routing messages.	Secure Routing
2005	Adjih, Raffo and Muhlethaler	Attacks Against OLSR: Distributed Key Management for Security	The paper presents the attack tree towards OLSR protocol, analyzes the possible attacks, and proposes a security architecture to secure OLSR.	Secure Routing
2005	Cai, Pan and, Shen and Mark	Peer Collaboration in Wireless Ad Hoc Networks	The paper applies IBC to peer collaboration, and uses Identity-Based signature and verification mechanisms to achieve authentication and non-repudiation of commitment proposal messages and commitment confirmation messages	Peer Collaboration
2006	Chien and Lin	Identity-Based Key Agreement Protocol for Mobile Ad-hoc Networks Using Bilinear Pairing	The paper proposes a *Tripartite key agreement protocol* which allows three parties establish their session keys, and uses the *Hierarchical ternary tree* and bilinear map to establish the cell group key.	Key Management
2006	Hoeper and Gong	Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation	The paper proposes a scheme for key revocation and key renewal using Identity-Based scheme in MANETs.	Key Management
2006	Hoeper and Gong	Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks	The paper proposes a MANET-IDAKE scheme in which a KGC initializes all devices before they join the network and all tasks are performed by the network nodes themselves without any central KGC.	Key Management
2006	Saxena	Public Key Cryptography Sans Certificates in Ad Hoc Networks	The paper proposes a scheme of PKI for MANET analogous to Identity-Based cryptography with some claimed advantages. Unlike other ID-based schemes, the proposal is based on standard (discrete logarithm) assumptions.	PKI
2007	Hoeper and Gong	Preventing or Utilizing Key Escrow in Identity-Based Schemes Employed in Mobile Ad Hoc Network	The paper derives two adversary models for dishonest PKGs in MANETs, analyzes the attack probabilities and proposes contermeasures, also discusses the problem of utilizing key escrow.	Key Management

Table V. Summary of Applications of Identity-Based Cryptography in MANETs (cont'd II)

5. CONCLUSIONS AND FUTURE WORK

In this survey, we have studied major developments in Identity-Based cryptography, and the application of Identity-Based cryptography to MANETs in various areas. During this study, we realize that Identity-Based cryptography is a new and still developing technology. We also notice the drawbacks and challenges of Identity-Based cryptography which impose difficulties on its application to MANETs. The main concerns for this new technology in the literature are as follows:

In [Granger et al. 2006], Granger et al state that it is still hard to say whether pairing-based cryptosystems (the mainstream of Identity-Based cryptosystems) will be able to provide satisfactory security and efficiency as the desired level of security rises. They state that as the security requirements increase, the price one has to pay for the extra functionality will increase sharply.

They also identify some theoretical concern on the pairing-based systems – the BDHP is a new problem that has not been widely studied. It is closely related to the Diffiee-Hellman Problem (DHP) in the elliptic curve group. It follows that if one has an algorithm for the DHP on the curve, one can immediately solve the BDHP as well. Hence it was a source of concern that security dependeds on the presumed intractability of the DHP rather than the more natural and more extensively studied Discrete Log Problem (DLP).

Another concern for pairing-based cryptosystems is from Verheul's discovery [Verheul 2004] which shows an example in which the DHP is efficiently solvable. The author further states if a Verheul homomorphism might some day be constructed, even if it were constructed just for the class-VI supersingular elliptic curves, that would be enough to render all pairing-based cryptosystems completely insecure.

In [Dutta et al. 2004], Dutta lists some disadvantages of identity-based systems: (1) the PKG knows Bob's private key, i.e. key escrow is inherent in the system which for some applications may be a serious problem, (2) Bob has to authenticate himself to it's PKG in the same way as he would authenticate himself to a certifying authority (CA), (3) Bob's PKG requires a secure channel to send Bob his private key, (4) Bob has to publish his PKG's public parameters and Alice must obtain these parameters before sending an encrypted message to Bob.

In [Boneh et al. 2005], Boneh et al notice that for all existing HIBE systems, the proof of full security degrades exponentially in the hierarchy depth. They state it is an open problem to construct a HIBE system where security does not degrade exponentially in the hierarchy depth.

In [Chen et al. 2004], Chen et al identify an open problem to design an ID-based group signature scheme from bilinear pairings with one key pair [8]. It is a drawback that a user should have a new key pair for each message if he wants to sign many message. In [Bellare et al. 2003], Bellare, Micciancio and Warinschi provide theoretical foundations for the group signature primitive. How to design an ID-based signature scheme under such foundation is another open problem.

[8]Group signature, introduced by Chaum and van Heijst [Chaum and van Heyst 1991], allows any member of a group to sign on behalf of the group. Anyone can verify the signature with a group public key while no one can know the identity of the signer except the Group Manager. Further, it is computational hard to decide whether two different signatures were issued by the same member.

Studies on these security concerns and challenges will be the future work on Identity-Based cryptography schemes and their applications.

ACKNOWLEDGMENTS

I would like to thank Dr. Richard A. Frost for his instruction on conducting a literature review and survey, thank Dr. Akshai K. Aggarwal for his suggestions on this topic.

REFERENCES

Adjih, C., Raffo, D., and Muhlethaler, P. 2005. Attacks against OLSR: Distributed key management for security. In *Proc. OLSR Interop and Workshop*. 1–7.

Al-Riyami, S. and Paterson, K. 2003. Certificateless public key cryptography. In *Advances in Cryptology – ASIACRYPT*. LNCS, vol. 2894. Springer-Verlag, 452–473.

Baek, J. and Zheng, Y. 2004. Identity-based threshold decryption. In *PKC: International Workshop on Practice and Theory in Public Key Cryptography*. LNCS, vol. 2947. Springer-Verlag, 262–276.

Balfanz, D., Smetters, D., Stewart, P., and Wong, H. 2002. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proc. Symp. Network and Distributed Systems Security*. Internet Society, 23–35.

Bellare, Micciancio, and Warinschi. 2003. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *Advances in Cryptology – EUROCRYPT*. LNCS, vol. 2656. Springer-Verlag, 614–629.

Bobba, R., Eschenauer, L., Gligor, V., and Arbaugh, W. 2003. Bootstrapping security associations for routing in mobile ad-hoc networks. In *IEEE Global Telecommunications Conference 2003*. Vol. 3. IEEE Computer Society Press, 1511–1515.

Bohio, M. and Miri, A. 2004a. Authenticated secure communications in mobile ad hoc networks. In *Proceedings of Canadian Conference on Electrical and Computer Engineering*. Vol. 3. IEEE Computer Society Press, 1689–1692.

Bohio, M. J. and Miri, A. 2004b. An authenticated broadcasting scheme for wireless ad hoc network. In *CNSR*. IEEE Computer Society, 69–74.

Bohio, M. J. and Miri, A. 2004c. Efficient identity-based security schemes for ad hoc network routing protocols. *Ad Hoc Networks 2,* 3, 309–317.

Boneh and Franklin. 2001. Identity-based encryption from the weil pairing. In *Proceedings of Crypto 2001*. LNCS, vol. 2139. Springer-Verlag, 213–219.

Boneh, D. and Boyen, X. 2004. Efficient selective-ID secure identity-based encryption without random oracles. In *Advances in Cryptology – EUROCRYPT*. LNCS, vol. 3027. Springer-Verlag, 223–238.

Boneh, D., Boyen, X., and Goh, E.-J. 2005. Hierarchical identity based encryption with constant size ciphertext. In *Advances in Cryptology – EUROCRYPT*. LNCS, vol. 3494. Springer-Verlag, 440–456.

Boneh, D., Gentry, C., Lynn, B., and Shacham, H. 2003. Aggregate and verifiably encrypted signatures from bilinear maps. In *Advances in Cryptology – EUROCRYPT ' 2003*. LNCS, vol. 2656. Springer-Verlag, 416–432.

Boneh, D., Lynn, B., and Shacham, H. 2001. Short signatures from the weil pairing. In *Advances in Cryptology – ASIACRYPT*. LNCS, vol. 2248. Springer-Verlag, 514–532.

Boyd, Mao, and Paterson. 2004. Key agreement using statically keyed authenticators. In *International Conference on Applied Cryptography and Network Security (ACNS)*. LNCS, vol. 3089. Springer-Verlag, 248–262.

Boyen, X. 2003. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In *Proceedings of Crypto*. LNCS, vol. 2729. Springer-Verlag, 383–399.

Cai, L., Pan, J., Shen, X., and Mark, J. W. 2005. Peer collaboration in wireless ad hoc networks. In *NETWORKING 4th International IFIP-TC6 Networking Conference Proceedings*,

R. Boutaba, K. C. Almeroth, R. Puigjaner, S. X. Shen, and J. P. Black, Eds. LNCS, vol. 3462. Springer-Verlag, 840–852.

Cha, J. and Cheon, J. 2003. An identity-based signature from gap diffie-hellman groups. In *PKC: International Workshop on Practice and Theory in Public Key Cryptography*. LNCS, vol. 2567. Springer-Verlag, 18–30.

Chai, Z.-C., Cao, Z.-F., and Zhou, Y. 2007. Efficient id-based multi-decrypter encryption with short ciphertexts. *Journal of Computer Science and Technology 22,* 1 (Jan.), 103–108.

Chaum, D. and van Heyst, E. 1991. Group signatures. In *Advances in Cryptology – EUROCRYPT*. LNCS, vol. 547. Springer-Verlag, 257–265.

Chen, L. and Kudla, C. 2003. Identity based authenticated key agreement protocols from pairings. Tech. Rep. HPL-2003-25, Hewlett Packard Laboratories. Feb. 12.

Chen, X., Zhang, F., and Kim, K. 2004. New ID-based threshold signature scheme from bilinear pairings. In *INDOCRYPT: International Conference in Cryptology in India*. LNCS, vol. 3348. Springer-Verlag, 371–383.

Chien, H.-Y. and Lin, R.-Y. 2006. Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing. In *SUTC*. IEEE Computer Society, 520–529.

Cocks, C. 2001. An identity based encryption scheme based on quadratic residues. In *IMA Conference on Cryptography and Coding*. LNCS, vol. 2260. Springer-Verlag, 217–252.

Crepeau, C. and Davis, C. 2003. A certificate revocation scheme for wireless ad hoc networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*. Vol. 1. 54–61.

Crescenzo, D., Arce, and Ge. 2005. Threshold cryptography in mobile ad hoc networks. In *International Conference on Security in Communication Networks*. LNCS, vol. 3352. Springer-Verlag, 91–104.

Deng, H. and Agrawal, D. P. 2004. TIDS: threshold and identity-based security scheme for wireless ad hoc networks. *Ad Hoc Networks 2,* 3, 291–307.

Deng, H., Mukherjee, A., and Agrawal, D. P. 2004. Threshold and identity-based key management and authentication for wireless ad hoc networks. In *ITCC (1)*. IEEE Computer Society, 107–111.

Desmedt and Quisquater. Public-key systems based on the difficulty of tampering (is there a difference between DES and RSA?) (extended abstract). In *CRYPTO: Proceedings of Crypto*. Vol. 263. 111–117.

Desmedt, Y. 1994. Threshold cryptography. *European Transactions on Telecommunications 5,* 4 (July – Aug.), 449–457.

Desmedt, Y. and Frankel, Y. 1989. Threshold cryptosystems. In *CRYPTO: Proceedings of Crypto*. LNCS, vol. 435. Springer-Verlag, 307–315.

Du, X., Wang, Y., Ge, J., and Wang, Y. 2003. Id-based authenticated two round multi-party key agreement. Cryptology ePrint Archive, Report 2003/247. Available at "http://eprint.iacr.org/2003/247".

Dutta, R., Barua, R., and Sarkar, P. 2004. Pairing-based cryptographic protocols: A survey. Cryptology ePrint Archive, Report 2004/064. Available at "http://eprint.iacr.org/2004/064".

Feldman, P. 1987. A practical scheme for non-interactive verifiable secret sharing. In *28th Symposium on Foundations of Computer Science*. IEEE, 427–437.

Gentry. 2003. Certificate-based encryption and the certificate revocation problem. In *Advances in Cryptology – EUROCRYPT*. LNCS, vol. 2656. Springer-Verlag, 272–293.

Gentry, G. and Silverberg, A. 2002. Hierarchical ID-based cryptography. In *Advances in Cryptology – ASIACRYPT*. LNCS, vol. 2501. Springer-Verlag, 548–566.

Granger, R., Page, D., and Smart, N. 2006. High security pairing-based cryptography revisited. In *Algorithmic Number Theory Symposium VII*. LNCS, vol. 4076. Springer-Verlag, 480–494.

Hess, F. 2002. Exponent group signature schemes and efficient identity based signature schemes based on pairings. Cryptology ePrint Archive, Report 2002/012. Available at "http://eprint.iacr.org/2002/012".

Hess, F. 2003. Efficient identity based signature schemes based on pairings. In *SAC: Annual International Workshop on Selected Areas in Cryptography*. LNCS, vol. 2595. Springer-Verlag, 310–324.

Hoeper, K. and Gong, G. 2005a. Identity-based key exchange protocols for ad hoc networks. In *Proceedings of Canadian Workshop on Information Theory*. 127–130.

Hoeper, K. and Gong, G. 2005b. Limitations of key escrow in identity-based schemes in ad hoc networks. In *Proceedings of First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. 403–405.

Hoeper, K. and Gong, G. 2006a. Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation. Report 2006-04, University of Waterloo.

Hoeper, K. and Gong, G. 2006b. Key revocation for identity-based schemes in mobile ad hoc networks. In *Proceedings of 5th International Conference on AD-HOC Networks and Wireless*. LNCS, vol. 4104. Springer-Verlag, 224–237.

Hoeper, K. and Gong, G. 2007. Preventing or utilizing key escrow in identity-based schemes employed in mobile ad hoc network. *Int. J. of Security and Networks (IJSN),*. to be published.

Huang, Y.-M. and Lin, H.-Y. 2003. Information service on scalable ad-hoc mobile wireless networks. In *Proceedings of Computer Networks and Mobile Computing 2003*. Vol. 20. 190–196.

Hubaux, J.-P., Buttyán, L., and Capkun, S. 2001. The quest for security in mobile ad hoc networks. In *MobiHoc*. ACM, 146–155.

jacques Quisquater, J. 2003. New identity based signcryption schemes from pairings. Cryptology ePrint Archive, Report 2003/023. Available at "http://eprint.iacr.org/2003/023".

J.Kong, Zerfos, P., Luo, H., and Zhang, L. 2001. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proc. IEEE ICNP*. Vol. 11. 251–260.

Joux, A. 2000. A one round protocol for tripartite diffie-hellman. In *ANTS IV*. LNCS, vol. 1838. Springer-Verlag, 385–394.

Khalili, A., Katz, J., and Arbaugh, W. A. 2003. Toward secure key distribution in truly ad-hoc networks. In *SAINT Workshops*. IEEE Computer Society, 342–346.

Kong, J., Luo, H., Xu, K., Gu, D. L., Gerla, M., and Lu, S. 2002. Adaptive security for multilevel ad hoc networks. *Wireless Communications and Mobile Computing 2,* 5, 533–547.

Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., and Yoo, S. 2004. Secure key issuing in ID-based cryptography. In *Proceedings of the second workshop on Australian information security, Data Mining and Web Intelligence, and Software Internationalisation*. Australian Computer Society, Inc., 69–74.

Lee, W. and Sriborrirux, W. 2004. Optimizing authentication mechanisms using ID-based cryptography in ad hoc wireless mobile networks. In *Proc. of International Conference on Information Networking, Networking Technologies for Broadband and Mobile Networks*. LNCS, vol. 3090. Springer-Verlag, 925–934.

Lee, Y.-H., Kim, H., Chung, B., Lee, J., and Yoon, H. 2003. On-demand secure routing protocol for ad hoc network using id based cryptosystem. In *Proc. Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*. IEEE Press, 211–215.

Li, G. and Han, W. 2005. A new scheme for key management in ad hoc networks. In *Networking - ICN 2005, 4th International Conference on Networking Proceedings, Part II*. LNCS, vol. 3421. Springer-Verlag, 242–249.

Lin, H.-Y., Huang, Y.-M., and WANG, T.-I. 2005. Resilient cluster-organizing key management and secure routing protocol for mobile ad hoc networks. In *Proceedings of IEICE Transactions on Communications*. Vol. E88-B. 3598–3613.

Luo, H., Zerfos, P., Kong, J., Lu, S., and Zhang, L. 2002. Self-securing ad hoc wireless networks. In *ISCC*. IEEE Computer Society, 567–574.

Lynn, B. 2002. Authenticated identity-based encryption. Cryptology ePrint Archive, Report 2002/072. Available at "http://eprint.iacr.org/2002/072".

Maurer and Yacobi. 1991. Non-interactive public-key cryptography. In *Advances in Cryptology – EUROCRYPT*. LNCS, vol. 547. Springer-Verlag, 498–507.

Montenegro, G. and Castelluccia, C. 2002. Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses. In *NDSS*. The Internet Society, 1–13.

Oh, J., Lee, K., and Moon, S.-J. 2005. How to solve key escrow and identity revocation in identity-based encryption schemes. In *ICISS*, S. Jajodia and C. Mazumdar, Eds. LNCS, vol. 3803. Springer-Verlag, 290–303.

Park, B.-N. and Lee, W. 2005. ISMANET: A secure routing protocol using identity-based signcryption scheme for mobile ad-hoc networks. *IEICE Transactions on Communications e88-b*, 2548–2556.

Park, B.-N., Myung, J., and Lee, W. 2004. ISSRP: A secure routing protocol using identity-based signcryption scheme in ad-hoc networks. In *Proceedings of Parallel and Distributed Computing: Applications and Technologies, 5th International Conference 2004*, K.-M. Liew, H. Shen, S. See, W. Cai, P. Fan, and S. Horiguchi, Eds. LNCS, vol. 3320. Springer-Verlag, 711–714.

Park, B.-N., Myung, J., and Lee, W. 2005. LSRP: A lightweight secure routing protocol with low cost for ad-hoc networks. In *Proceedings of International Conference on Convergence in Broadband and Mobile Networking*. LNCS, vol. 3391. Springer-Verlag, 160–169.

Paterson, K. G. 2002. ID-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, Report 2002/004. Available at "http://eprint.iacr.org/2002/004".

Rhee, K. H., Park, Y.-H., and Tsudik, G. 2005. A group key management architecture for mobile ad-hoc wireless networks. *J. Inf. Sci. Eng 21,* 2, 415–428.

Sakai, R., Ohgishi, K., and Kasahara, M. 2000. Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security*. 26–28.

Saxena, N. 2006. Public key cryptography sans certificates in ad hoc networks. In *Applied Cryptography and Network Security, 4th International Conference Proceedings*, J. Zhou, M. Yung, and F. Bao, Eds. LNCS, vol. 3989. Springer-Verlag, 375–389.

Shamir. 1984. Identity-based cryptosystems and signature schemes. In *CRYPTO: Proceedings of Advances in Cryptology*. LNCS, vol. 196. Springer-Verlag, 47–53.

Shamir, A. 1979. How to share a secret. *Communications of the ACM 22,* 11, 612–613.

Shoup, V. and Gennaro, R. 2002. Securing threshold cryptosystems against chosen ciphertext attack. *JCRYPTOL: Journal of Cryptology 15*, 75–96.

Song, J., Kim, H., Lee, S., and Yoon, H. 2005. Security enhancement in ad hoc network with id-based cryptosystem. In *Proceedings of the 7th International Conference on Advanced Communication Technology*. IEEE Computer Society Press, 372–376.

Tanaka, H. 1987. A realization scheme for the identity-based cryptosystem. In *Advances in Cryptology—CRYPTO '87*, C. Pomerance, Ed. LNCS, vol. 293. Springer-Verlag, 340–349.

Tsujii, S. and Itoh, T. 1989. An ID-based cryptosystem based on the discrete logarithm problem. *IEEE Journal on Selected Areas in Communications 7,* 4 (May), 467–473.

Verheul, E. 2004. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *JCRYPTOL: Journal of Cryptology 17*, 277–296.

Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. 2004. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications 11,* 1, 38–47.

Zhang, P., Ye, C., Li, X., Cheng, Y., and Ma, X. 2005. Constant-round contributory group key agreement for ad hoc networks. In *Proceedings of the IEEE Wireless Communications, Networking and Mobile Computing*. Vol. 2. IEEE Computer Society Press, 1245–1248.

Zhang, Y., Liu, W., and Lou, W. 2005. Anonymous communications in mobile ad hoc networks. In *INFOCOM*. IEEE, 1940–1951.

Zhang, Y., Liu, W., Lou, W., Fang, Y., and Kwon, Y. 2005. Ac-pki: anonymous and certificateless public-key infrastructure for mobile ad hoc networks. In *Proceedings of the IEEE International Conference on Communications*. IEEE Computer Society Press, 3515–3519.

Zhou, L. and Haas, Z. J. 1999. Securing ad hoc networks. *IEEE Network 13,* 6, 24–30.