A Survey on Key Management of Identity-based Schemes in Mobile Ad Hoc Networks

Kuo Zhao, Longhe Huang, Hongtu Li, Fangming Wu, Jianfeng Chu, and Liang Hu
Jilin University, Chang Chun 130012, China
Email: zhaokuo@jlu.edu.cn, ccsthlh@163.com, li_hongtu@hotmail.com, 4464532@qq.com, chujf@jlu.edu.cn, 525108836@qq.com

***Abstract*—**In mobile ad hoc networks (MANETs), the research on key management of identity-based scheme is attracting more and more attention. In this paper, we study on four types of identity-based schemes which resist key escrow problem at different degrees, and introduce several schemes for each type. Then, we give an overview of the characteristics of their key management, and made a summary of key generation and distribution. Subsequently, to build a more secure identity-based scheme for MANET, we recommend some techniques to improve security and availability of its key management. Finally, we point out some problems of identity-based schemes in MANETs, which are not addressed and we will explore in the future.

***Index Terms*—**MANETs, identity-based cryptography, key management

I. Introduction

A mobile ad hoc network (MANET) is a cooperative wireless network of mobile hosts (which we call nodes or users) that can communicate with each other without any centralized administration or preexisting infrastructure [1], [2]. The nodes of network operate both as communication end points as well as routers, enabling multi-hop wireless communication. Because of the rapidity, self-organizing, self-configuring and low cost for forming network, MANETs have attracted a lot of attention from both the research and industry communities, which are extensively employed in military, vehicle networks, disaster relief and emergency, where geographical or terrestrial constraints demand totally distributed networks.

However, due to the wireless, bandwidth-limited, resource-constrained, and dynamic nature, MANETs are more vulnerable to security attacks [3] than their wired counterparts. Wireless communication, for example, is open to interference and interception, and malicious nodes might create, alter, or replay routing information to interrupt network operation. Moreover, malicious nodes may inject bogus data into the network to consume its scarce resources, and selfish nodes can drop data packets of other nodes.

Cryptographic schemes with key management are employed to provide a general design framework for secure MANETs. Traditional cryptographic systems can be divided into symmetric and asymmetric ones, depending on the way they use keys [4]. In symmetric schemes, the secret keys must be shared either by a secure pre-established channel or before network formation. If an attacker compromises the symmetric key of a group of users, then all encrypted messages for that group will be exposed. Therefore, traditional symmetric schemes are difficult to apply in MANETs. [5] The key management schemes of traditional asymmetric schemes are usually based on Public Key Infrastructure (PKI). The success of certificate-based PKI depends on the availability and security of a Certificate Authority (CA), a central control point that everyone trusts. In a MANET, nodes have non-negligible probability to be compromised for the resource limitations of wireless devices and relatively poor physical protection. Once CA is compromised, the security of the network would be subverted. Another obstacle of using PKI's in MANETs is the heavy overhead of transmission and storage of Public Key Certificates (PKCs). [6]

As a powerful alternative to certificate-based PKI, identity-based cryptography (IBC) [7], [8] allows public keys to be derived from entities' known identity information, thus there is no requirement of CA and PKCs. Recent decade, IBC has attracted more and more attention from researcher, and a number of identity-based schemes [9]-[12] have been proposed. The advantages of identity-based key management: reducing the cost of storage, computation and communication, make IBC more suitable for bandwidth-limited and resource-constrained MANETs.

An identity-based scheme needs a Private Key Generator (PKG) to identify the user's ID and compute private key, which results single point of failure. Furthermore, there exits key escrow problem (inherent in identity-based cryptosystems), since PKG knows the private keys of all nodes. Similar to the CA in PKI, once PKG is not credible, system won't be able to ensure communication non-repudiation if the compromised PKG pretends to be user to send messages. In order to

Manuscript received June 15, 2013; revised October 24, 2013.
This work was supported in part by the National High Technology Research and Development Program of China (Grant No. 2011AA010101), and the National Natural Science Foundation of China (Grant No. 61103197).
Corresponding author email: 525108836@qq.com.
doi:10.12720/jcm.8.11.768-779

eliminate or reduce the risks of key escrow problem, several revised types of identity-based schemes have been made using multiple authority approaches. But meanwhile, they also cause some other new problems. For example, traditional threshold identity-based schemes [13] weaken the key escrow problem by distributing the PKG's service to multiple nodes, but they need to have a trust authority (TA) and provide the secure distribution of secret shares.

In this survey, we study on four types of identity-based key management schemes which resist key escrow problem at different degrees in MANETs: traditional threshold identity-based schemes, Secrete Shares as Private Keys (SSPK) identity-based schemes, certificateless schemes, and hierarchical identity-based schemes. Then, we discuss the approaches, strengths, and weaknesses of key management of these schemes, and provide a comparison between their main features.

The remainder of this paper is organized as follows: Section II presents an overview of some background knowledge. Next, we describe the multiple identity-based key management schemes in section III, and then we present a comprehensive picture and discuss their strengths and weaknesses in following section. The final section draws our conclusion.

II. Preliminaries

In this section, we start from reviewing the brief history and basic concepts of IBC, and subsequently introduce an identity-based encryption (IBE) scheme and an identity-based signature (IBS) scheme based on the bilinear pairing, a computational primitive widely used to build up various identity-based cryptographic schemes in the current literature. Then we will present the basic idea of threshold cryptography, and describe one classical (t, n) threshold cryptography.

A. Identity-Based Cryptography

As mentioned earlier, in the IBC, the public key/secret key pair is generated by a PKG service, and the public key based on the own identity is assumed to be known by everyone. The idea of IBC was first proposed by Shamir [8] in 1984. Over years, a number of researchers tried to propose secure and efficient identity based encryption algorithms, but with little success. Boneh and Franklin [7] presented first fully functional, efficient and provably secure IBE scheme in 2001. At the same year, Boneh, Lynn and Shacham [14] proposed a basic IBS scheme using pairing.

In an IBE scheme, the sender can use the receiver's identity of public key to encrypt message, and the receiver can decrypt the ciphertext by his own private key obtained from the PKG according to his identity. The functions that compose a generic IBE are specified by the following four randomized algorithms [13], [15]. (Fig. 1 illustrates a schematic outline of an IBE scheme.)

- Setup: takes a security parameter and returns system master private key *SK* and public key *PK*.
- Extract: takes system parameters, master private key, and an identity as input, and returns a secret private key *sk* corresponding to the identity.
- Encrypt: takes the master public key, the public key of the receiver node (derived from its identity), and the message as input, and returns the corresponding ciphertext.
- Decrypt: takes the master public key, a ciphertext and the personal private key as input, and returns the decrypted message.

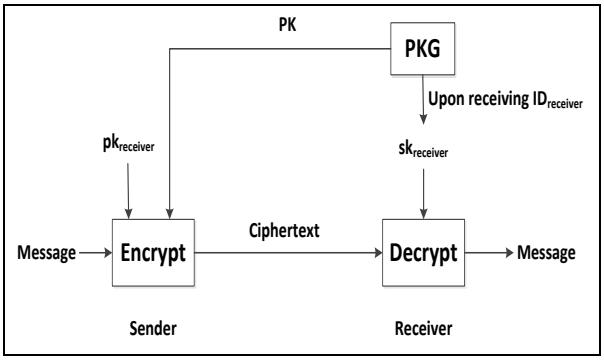

Figure 1. Identity-based encryption

In an IBS scheme, the singer first obtains a signing private key associated with its own identity from the PKG. It then signs a message using the private key, and the verifier verifies the signature using the signer's public key. An IBS scheme can also be described using four randomized algorithms [14], [15]: Setup, Extract, Signing, and Verification. The former two steps are same to Setup and Extract of an IBE scheme. (Fig. 2 illustrates a schematic outline of an IBS scheme.)

- Signing: uses own private key to create a signature on the message.
- Verification: takes the master public key, the signature, the message and the public key of sender as input, checks whether the signature is a genuine signature on the message. If it is, returns "Accept". Otherwise, returns "Reject".

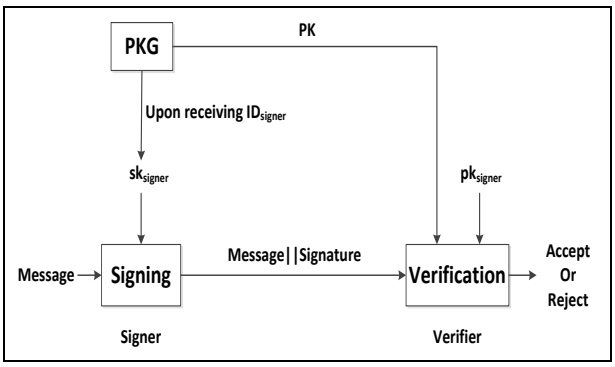

Figure 2. Identity-based signature

Currently, most of IBC schemes for MANETs are based on the bilinear pairing technique and assumptions of hard problems in elliptic curves. Let G_1 and G_2 denote two groups of the same large prime q, where G_1 is an

additive group that consists of points on elliptic curve and G_2 is a multiplicative group on a finite field. A bilinear pairing is a computable bilinear map between two groups. Two pairings have been studied for cryptographic use. The admissible bilinear map, denoted by $e: G_1 \times G_2 \rightarrow G_2$, has the following properties.

- Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, where $P, Q \in G_1$ and $a, b \in Z_q^*$
- Non-degenerate: there exit $P, Q \in G_1$, such that $e(P, Q) \neq 1$
- Computable: there is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$

The most frequently used assumptions are CDHP assumption and BDHP assumption, which means there is no polynomial time algorithm to solve CDH problem or BDH problem with non-negligible probability.

- Computational Diffie-Hellman (CDH) problem: for $\forall a, b \in Z_q^*$, given $P, aP, bP \in G_1$, compute $abP \in G_1$.
- Bilinear Diffie-Hellman (BDH) problem: for $\forall a, b, c \in Z_q^*$, given $P, aP, bP, cP \in G_1$, compute $e(P, P)^{abc} \in G_2$.

B. Threshold Cryptography

In (*t*, *n*) threshold cryptography [16], [17], a cryptographic action divides a secret to *n* shareholders. Any *t* or more shareholders can combine their shares to deduce the secret. But any combination of *t*-1 shares does not yield any significant information about the secret. So, in such a way, the cryptographic action can be performed if and only if at least a certain number of parties collaborating. By this principle, in identity-based and threshold distributed key management scheme, the PKG's service is distributed to multiple parties [13]. More details, the master private key *SK* is shared by n nodes in a (*t*, *n*) threshold fashion. Each of them holds a unique secret share of the master private key *SK*, and no one is able to reconstruct the master private key based on its own information. Any *t* or more nodes among them can reconstruct the mater private key jointly, whereas it is infeasible for at most *t*-1 nodes to do so, even by collusion.

One classical (*t*, *n*) threshold cryptography [18] was proposed by Shamir in 1979, which is based on polynomial interpolation. To distribute a secret s among n users, a trust authority chooses a large prime *q* and randomly selects a random *t*-1 degree polynomial *f*(*x*), with *f*(0)=*SK*. The trust authority computes each user's share using $S_i = f(i) \bmod q$ and securely sends the share S_i to user *i*. Then any *t* or more shareholders can reconstruct the secret using the Lagrange interpolation by $S = \sum_{i=1}^{k} S_i l_i \bmod q$, where $l_i = \prod_{j=1, j\neq i}^{k} \frac{j}{j-i}$ is the Lagrange coefficient.

III. Identity-based Key Management Schemes

To tackle the inherent key escrow problem of IBC, several proposals have been made using multiple approaches. Many identity-based schemes for MANETs combine Shamir's threshold scheme to distribute the PKG service to an aggregation of nodes (PKGs), then no single node knows the private keys of all nodes, thus the key escrow problem of PKG is weakened. Actually, Shamir's threshold cryptography is suggested earlier then IBC to secure ad hoc networks by Zhou *et al*. [19] in 1999. Khalili *et al*. [13] suggest a mechanism that combines 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. In their system, IBC primarily provides efficiency gains, and threshold cryptography provides resilience and robustness.

However, Shamir's threshold secret sharing scheme has two major weaknesses. First, the scheme needs a TA to distribute a secret to users. Second, the scheme does not detect the distributed erroneous shares and the false shares provided by some compromised users. Deng *et al*. [20], [21] proposed a secret sharing scheme without TA, instead, users choose the secret and distribute it among themselves, based on the work [22]. To testify the correctness of the shares, a SSPK identity-based scheme [23] using Verifiable Secret Sharing (VSS) [24] was proposed. What's more, in the threshold secret sharing phase of [23], nodes use secret VSS shares as private keys, which is different from traditional threshold identity-based schemes, and that's why we put it as a separate type. Still, given enough time an adversary could corrupt enough serve users (*t* PKGs) and obtain their shares to reconstruct the secret. To defend against such mobile attacks [25], a proactive secret sharing scheme [26] using shares refreshing to compute new shares and remove the old shares was proposed.

Although above threshold identity-based schemes can weaken the key escrow problem at server level. There still remain risks of *t* PKGs being compromised. Hence, the key escrow problem is not completely addressed. Al-Riyam and Paterson [27] first proposed a certificateless public key cryptography (CL-PKC) that combines the advantages of IBC and PKI and overcomes the key escrow limitation of IBC. We will study on some certificateless schemes for MANETs [28], [29], [30] because certificateless-based schemes enjoy a number of features of IBC, though they are not purely identity-based.

Besides multiple identity-based schemes for flat MANETs, there are also some hierarchical identity-based schemes [31], [32], [33] for hierarchical MANETs. Considering the spatial concurrency constraints on nearby nodes sharing the same channel and the organization of the network may already be hierarchical in nature, so a hierarchical key management structure could serve well

for applications of lager scale or of hierarchy. The good news is that hierarchical identity-based schemes also allow key escrow free at server levels.

In the following part, we will describe above identity-based key management schemes more detailedly.

A. Traditional Threshold Identity-Based Schemes

In traditional threshold identity-based schemes, the parameters of the cryptosystem, like master public/private key pair, will be, generally speaking, established by an online/offline TA or by other way before network deployment. The master public key *PK* is known to all nodes in the network, whereas the secret private key *SK* is divided into *n* shares S_1, S_2, ..., S_n, one share for each server node in a t-out-of-n threshold manner. Each of server nodes holds a unique secret share of the master private key *SK*, and no one is able to reconstruct the master private key based on its own information. These multiple server nodes act as the threshold PKGs of an ID-based scheme, and any *t* server nodes can work together to issue personal secret private keys to nodes (including themselves) in MANETs based on their identities and key issuance policy, whereas it is infeasible for at most *t*-1 nodes to do so, even by collusion.

Instead of assuming that prior keying material or trust/security associations (TA) exist, Khalili *et al*. establish these at the time of network formation. In more detail, they propose that (at the time of network formation) the participating nodes generate a master public key *PK* in a distributed fashion. The master secret key *SK* will be shared in a t-out-of-n threshold manner by this initial set of *n* nodes called PKGs.

At the time of network formation, the initial nodes decide on a mutually acceptable set of security parameters, including a threshold *t* of key service nodes, the number (*n*) and identity of key service nodes, particular parameters of underlying schemes (*e.g.* key lengths), and a policy for key issuance. This initial set of nodes will generate the master public/private keys in a distributed manner such that fewer than *t* nodes cannot recover the master secret key. The master public key is given to all members of the network when they join. Usually, an identity can be something present in transmitted messages, like the network layer (or MAC) address, and all nodes in the network can use their identities as their personal public keys. When a new node join the network, it presents its identity or public key and any extra material specified by the key issuance policy to *t* or more PKGs providing the PKG service, then it will receives a share of their personal private key from each of them. The new joining node can then compute its personal private key using the t shares.

They recommend Boneh-Franklin scheme [7] as IBE scheme and Cha and Cheon [10] scheme as IBS scheme. These two schemes use similar elliptic-curve groups, and hence can be combined for greater efficiency in a relatively straightforward manner. All subsequent communications in their scheme are encrypted and decrypted using the master public key and the ID of the recipient.

In the Khalili *et al*. scheme, however, technical details of key generation are not given. Lots of identity-based schemes [34]-[36] in MANET are proposed based on the idea of their scheme. Among them, Deng *et al*. [20], [21] make a detailed implementation of [13] idea and propose a distributed key generation (distribution) and authentication approach by deploying the concepts of IBC and threshold secret sharing. In these schemes, key generation provides the network master key pair and the public/private key pair of each node in a distribute way. Key generation consists of three components: master key generation, distributed private key generation, new master key share creation for new joining nodes.

Master key generation: The master key pair is computed collaboratively by the initial network nodes without constructing the master private key at any single node. This scheme is an extension to Shamir's secret sharing without the support of a TA. Each node *i* randomly chooses a secret x_i and a polynomial $f_i(x) = x_i + a_{i,1}x^2 + \ldots + a_{i,t-1}x^{t-1} \bmod q$ of degree *t*-1, such that $x_i = f_i(0)$, and the master private key $SK = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} f_i(0)$. Node *i* computes his sub-share ss_{ij} for node j as $ss_{ij} = f_i(j)$, $j=1,2...n$ and sends ss_{ij} securely to node *j*. After receiving *n*-1 sub-shares, node *j* computes its share of master private key as $S_j = \sum_{i=1}^{n} ss_{ij} = \sum_{i=1}^{n} f_i(j)$ and acts as a PKG node. Any coalition of *t* shareholders can jointly recover the secret as $\sum_{i=1}^{k} S_i l_i \bmod q = \sum_{i=1}^{n} x_i = SK$, where $l_i = \prod_{j=1, j\neq i}^{k} \frac{j}{j-i}$ is the Lagrange coefficient. After the master private key is shared, each shareholder publishes S_iP, then the master public key $PK = \sum_{i=1}^{n} S_iP$.

Private Key Generation: The requesting node *i* presents its public key pk_i and self-generated temporary public key pk_i-*temp* when it joins the network and sends private key generation request. Each of the *t* PKGs sends encrypted share $S_j \cdot pk_i$ to the requesting node using pk_i-*temp*. By collecting the *t* shares of its new private key, the requesting node would compute its new private key $sk_i = \sum_{j=1}^{t} S_j \cdot pk_i$. After the requesting node gets its new private key, it discards its temporary public/private key pair, and keeps the new key pair in its memory for the later authentication and communication.

Master key share creation for new joining nodes: Every new joining node will be the PKG service node, in

other word, these schemes fully distribute the functionality of PKG to the entire nodes of the network. After private key generation process, the requesting node *i* obtains its new private key. To initialize the share of master key for the requesting node, each PKG node *j* generates the partial shares $ss_{ji} = S_j \bullet l_j(i)$ for node *i*, where $l_j(i)$ is the Lagrange term. It encrypts the partial share using the temporary public key of requesting node and sends it to node *i*. Node *i* obtains its new share by adding the partial shares as $S_i = \sum_{j=1}^{t} ss_{j,i}$. After obtaining the share of master private key, the new joining node becomes a PKG service node and is available to provide PKG service to other new joining nodes.

In these schemes, the public key of node *i* is computed as $pk_i = H(ID_i \,||\, Expire\_time)$ or $pk_i = H(ID_i \,||\, MAC \,||\, Expire\_time)$. When the public key is expired, the node needs to obtain its new public key and update corresponding private key. The generated private keys are used for authentication, providing end-to-end authentication and confidentiality between the communicating nodes. If the authentication process succeeds, the two communicating nodes calculate a symmetric session key, which can be used for future data encryption/decryption. Ref. [20], [21] refer three authentication method: a sign-and-encryption procedure, in which digital signature [7] is used for the authentication of messages and encryption [37] is used for the confidentiality of messages; By modifying the identity-based cryptosystem slightly, the communicating nodes can generate a shared secret (session key) on both sides without additional key exchange [38]; The lightweight authentication and encryption is implemented by applying the concepts of identity-based signcryption [8] and one-way hash chain [39].

Instead of encrypting subshares of private key using temporary public key, Li *et al*. [26] suggest a signcryption scheme [40] to secure the subshares' transmission. Moreover, they use modified multicast protocol and key proxy technology to reduce traffic and increase safety of key management when nodes update their private keys or PKG server nodes refresh their shares of master private key. They detail three components of key management: (master) key generation, update of a node's private key, and share refreshing of server nodes.

Key Generation: At the initial time of the network, an offline TA generates system secret key *SK* and public key *PK*. Every initial node must contact TA and register its identity before entering the network. After TA authenticates identity of the node, it actes as PKG and generates private key of the node using system secret key and the node's identity. Then the private key of the node and the system public key are given to the node securely. TA chooses *n* nodes as online PKG server nodes (PKGs) according to abilities of the nodes. Then the master private key *SK* is shared by the *n* server nodes using an (*t*, *n*) threshold sharing scheme. In addition, the offline TA publishes a piece of verification information consisting of $S_i P$ for each server node *i* to check malicious PKG server nodes as we will show later. The offline TA will leave the network after key generation succeeds.

The lifetime of the network is divided up in time periods, where each time period consists of two phases, the operational phase and the share update phase. During the operational phase, all nodes including server nodes renew their private keys. During the share update phase, all server nodes compute new shares from old ones in collaboration. At the *j*-th time interval, node A uses ($ID_A||j$) as its public key, where "||" represents concatenation of strings.

Update of a node's private key: All server nodes form and maintain a few multicast groups according to location, and each group has more than *t* server nodes. Node A floods its RREQ (Routing REQuset) to find a route to the online PKG 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. Before time interval *j* expires, it sends its *PREQ* to *u* and *u* multicasts the *PREQ* to all server nodes in the same group. Each server node *i* having received the request computes a subshare of private key $S_i \cdot pk_A$ for the node A using its share of system secret key S_i, then it sends a *PREP* message containing the subshare to the key proxy *u*. Node *u* waits for some time and checks whether it has received *t* or more subshares from different server nodes. If it is true *u* will return to node A all these subshares in a single *PREP* packet. Then node A can compute a new valid private key using Lagrange interpolation as we can see before. Otherwise, node *u* will multicast the same *PREQ* again until the number of partial private keys received is larger than *t*. It is possible that a malicious server node *i* may return a false partial private key generated without using its share. To check the validity of partial key it receives from *i*, node A needs to check whether the equation $e(pk_A, S_i P) = e(S_i \cdot pk_A, P)$ holds.

Shares refreshing of server nodes: Each server nodes *i* randomly generates its sub-shares tuple $(S_{i1}, S_{i2}, S_{i3}, \ldots S_{it})$. Node *i* signcrypts every subshare $S_{i,k}$, $i \neq k$, with its own private key and the public key of server node *k*. The ciphertext is denoted as c_k. Shares refreshing information of server node *i* consists of a vector $(c_1, \ldots c_{i-1}, 0, c_{i+1}, \ldots c_n)$, and the shares refreshing information is sent using multicast. Every server node *j* in the same group can receive refreshing information from node *i*, and can only decrypt ciphertext c_j to recover S_{ij} and learn nothing about other subshare S_{ik}, $i \neq k$. After node *j* gets the sub-shares $(S_{1,j}, S_{2,j}, S_{3,j}, \ldots S_{t,j})$ from other server nodes in the same group, it can

compute the new share from the old share and its own share as $S_{j-new} = S_j + \sum_{i=1}^{t} S_{i,j}$.

They point out there are two methods for communicating nodes to create a secret session key: key agreement using IBS by two parts, and session key generated by one part.

This scheme relies on an offline TA to form a trust anchor, which improves security level of the network. The multicast group of PKGs is fundamental in the scheme, but a critical question remaining open in this work is how the multicast group is formed.

Schemes [13], [20], [21] conduct a distributed PKG and weaken the key escrow problem of PKG up to the threshold *t*, which means an adversary should corrupt at least *t* PKG service nodes in the worst case, if it wants to obtain the private keys of all nodes. Here, we denote the degree of resistance to key escrow (DRKE) of [13], [20], [21] is *t*. In [26], due to the new shares being independent of the old ones, the adversary cannot combine old shares with new shares to recover the secret. Thus, secret refreshing mechanism reduces the risk of mobile attacks and weakens the key escrow problem at higher level than [20], [21]. But the DRKE of [26] is also *t*.

B. SSPK Identity-Based Schemes

Saxena [23] proposes a scheme of public key cryptography for MANETs analogous to IBC above. They use a Verifiable Secret Sharing (VSS) [24] as a key distribution scheme, and the major difference from traditional threshold identity-based schemes, as we mentioned before, is that they use the secret shares as the private keys. In the proposed scheme the private keys are related (they are points on a polynomial of degree *t*-1) and each public key can be computed from the public VSS information and the node identifier. The usage of shares as private keys can also be viewed as a threshold-tolerant identity-based cryptosystem under standard discrete logarithm based assumptions.

They use Feldman's VSS based Shamir's threshold cryptography to share the master secret private key. A dealer chooses a secret sharing polynomial $f(x) = a_0 + a_1 x^2 + \ldots + a_{t-1} x^{t-1}$ in Z_q, where a_0 is the system secret key *SK*. The dealer also publishes commitments to the coefficients of the polynomial, as $w_i = g^{a_i} \bmod p$, for *i*=0, ⋯;*t*-1. These witnesses constitute the public key of the system. To join the network, a user *i* with a unique identifier (such as an email address) ID_i , receives from the dealer a secret share (treated as private key sk_i) $sk_i = S_i = f(ID_i) \bmod q$ over a secure channel. The public key $pk_i = g^{sk_i} \bmod p$ of node *i* can be computed by other user using the public key of the network and its identifier ID_i as $pk_i = \prod_{j=0}^{t-1} (w_j)^{ID_i^j} \bmod p$.

Now, any user can send encrypted messages to user *i* using its public key pk_i ,and user *i* can decrypt using its secret key sk_i as ElGamal encryption [41]. Similarly, user *i* can use sk_i to sign messages, which can be publicly verified using pk_i using Schnorr signature scheme [42]. Moreover, any two users *i* and user *j* can establish pairwise keys in a non-interactive version of the Diffie-Hellman pairwise key establishment protocol: user *i* computes $k_{i,j} = pk_j^{sk_i} \bmod p$, and user *j* computes $k_{ji} = pk_i^{sk_j} \bmod p$. Since $k_{ij} = k_{ji}$, a hash of k_{ij} can be used as a session key for secure communication between user *i* and user *j*.

In a VSS identity-based scheme, a trusted dealer provides each user with a secret value as the private key derived from the unique identifier of the user, and publishes the VSS information as its public key. 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 of [7] and IBS of [10], apart from the fact that our scheme becomes insecure if there is more than a threshold of collusions or corruptions. What's more, unlike other identity-based schemes, the proposed usage of shares as private keys is under standard discrete logarithm based assumptions, and that is much more efficient than these prior IBC schemes requiring costly computations (such as scalar point multiplications, map-to-point operations and bilinear mappings [7]) in elliptic-curves. But the dealer who holds the secret sharing polynomial can compute the private key of all nodes, so the key escrow problem is not addressed or weakened.

C. Certificateless Schemes

CL-PKC enjoys a number of features of IBC while without having the problem of key escrow. LV *et al.* [28], [29] present a virtual private key generator (VPKG)-based escrow-free certificateless public key cryptosystem for MANETs as a novel combination of certificateless and threshold cryptography. In their schemes, VPKGs collaboratively calculate the partial private key and send it to the node via public channel. The private key sk_i of node *i* is generated jointly by the VPKG and the node itself. Each of them has "half" of the secret information about sk_i.

In the initialization phase, an offline trust authority (TA) create some system parameters, and picks a secret key *SK* and a secret polynomial $f(x) = a_0 + a_1 x^2 + \ldots + a_{t-1} x^{t-1}$, where $a_0 = SK = f(0)$. Then TA distributes the secret shares $S_i = f(i)$, *i*=1,...,*n*, to the *n* virtual PKG nodes in an offline way. Then $PK = SK \cdot P$ is the public key of the system. After network initialized, TA leaves the network, and the distributed VPKGs will be in charge of calculating private keys for nodes.

A mobile node i picks a secret s_i for itself and selects a nearby server node, say u as its combiner (similar to key proxy). Then, node *u* finds other *t*-1 server nodes and sends ID_i (and public key pk_i) to them. When the combiner *u* receives all shares from the other *t*-1 server nodes via public channels, it can compute the partial private key and then sends the partial private key to the requesting node i.

In [28], the public key of node *i* is $pk_i = (H_1(PK, ID_i), H_1(ID_i))$. Node *i* computes $sk_i = SK \cdot H_1(PK, ID_i) + s_i \cdot H_1(ID_i)$ as its real private key, the first part $SK \cdot H_1(PK, ID_i)$ is obtained from the VPKGs by the public channel. The second part $s_i \cdot H_1(ID_i)$ is known only to the node itself. In [29], the public key of node *i* $pk_i = (s_i P, s_i PK)$. Node *i* computes $sk_i = s_i \bullet SK \cdot H_1(ID_i, pk_i)$ as its real private key and $B_i = e(sk_i, P)$ for verifying the authenticity of the public key pk_i. Those two schemes respectively introduce how the above key pairs <pk_i,sk_i>are used to perform encryption/decryption using the Boneh-Franklin scheme[7].

LV *et al*. bind the public key of node *i* with its identity and its partial private key respectively, which raises their schemes to the same trust level as is enjoyed in a traditional PKI. Furthermore, with this binding, it does not need to keep the partial private keys secret, and the VPKG can send them back to the users via public channels.

Li *et al*. [30] also present a novel distributed key management scheme, a combination of certificateless public key cryptography and threshold cryptography. They point that each public/private key pair is both node-specific and phase-specific and node A's key pair valid only during phase p_i is denoted by $< pk_{A,p_i}, sk_{A,p_i} >$. Each of pk_{A,p_i} and sk_{A,p_i} is comprised of a node-specific element and a phase-specific element common to all nodes.

The network initialization and key generation is similar to LV *et al*.'s schemes. But the public key of node A during phase p_i is $pk_{A,p_i} = (pk_A, pk_{p_i}) = ((s_A \bullet SK \cdot P, s_A P), H_1(salt_i))$ and the corresponding private key is $sk_{A,p_i} = (sk_A, sk_{p_i}) = (s_A \bullet SK \cdot H_1(ID_A), s_A \bullet SK \cdot H_1(salt_i))$, where s_A is A's partial secret, $salt_i$ is a unique binary string as phase p_i's salt. $< pk_{p_i}, sk_{p_i} >$ varies across key-update phases, while $< pk_A, sk_A >$ remains unchanged during network lifetime and should be kept confidential to A itself.

They also employ key revocation and key update in the scheme and describe a key agreement to compute a shared session key.

In certificateless schemes, the private key of the user is generated collaboratively by the user and the VPKGs that calculates one part of a user's private key and sends it to the user via public channel. Each has half of the private information about the private key of the user. Thus there is no private key secure distribution problem. In addition, the user's partial private key is known only to the user itself, therefore there is no key escrow problem.

D. Hierarchical Identity-Based Schemes

Usually, a MANET is assumed to be homogeneous or flat, where all nodes have the same communication capabilities. A recent theory study in [43] presents the throughput bounds of homogeneous MANETs. The limitation is fundamentally due to the spatial concurrency constraints on nearby nodes sharing the same channel. These results strongly suggest that we should consider a hierarchical structure to solve the MANETs problem [44]. Recently, hierarchical ad hoc networks have been presented as an alternative topology to homogeneous ad hoc topologies. Initial measurements indicate that the hierarchical approach has better performance than homogeneous ad hoc network [45]. In addition, a hierarchical key management scheme could serve well for some special applications, e.g. military where the organization of the network may already be hierarchical in nature. In hierarchical key management, an upper level TA/PKG needs only distribute keys to the layer below it, and the distribution process continues until all the end-nodes get their secret keys from the layer above them. This hierarchy of PKG nodes greatly reduces the workload on master servers and allows key escrow free at server levels [27].

The first hierarchical identity-based encryption was proposed in [46]. The scheme is only two levels where a pairing-based scheme is placed at the top level and a polynomial-based scheme is at the second level. Their encryption functionality can support key agreement, but it requires user interaction. Gennaro *et al*. [31] reverses the order, using the polynomial scheme for all the top levels and the pairing-based scheme only for the leaves to supports the non-interactive property.

Gennaro *et al*. propose that an authenticated key agreement protocol for MANETs should have the four functional properties: non-interactive to save on bandwidth, identity-based to save on coordination and support ad-hoc communication, hierarchical to allow for flexible provisioning of nodes, and be fully resilient against compromise of any number of leaf nodes and resilient against compromise of a "threshold" of nodes in the upper levels.

Their goal is to build a hierarchical identity-based key agreement scheme that has all the above functional properties and is secure in a strong sense. Their scheme is a combination of linear hierarchical schemes with the non-interactive identity-based key-agreement scheme. It describes two special linear hierarchical schemes:

multivariate polynomials [47] scheme and subset-based key pre-distribution [48] scheme. In their scheme, each leaf can compute the shared key between other peer leaf node from its own secret key, its peer's identity, and potentially some other public information.

They discuss three trade-offs that one can make when choosing a key-agreement scheme for a particular application, that is "Set threshold value", "Polynomials vs. Subsets" and "Choosing the curves". They also implement the key-generation by the root and key-delegation between internal nodes.

Unlike other hierarchical key management schemes that rely on parent nodes to act as the PKG who supplies the private key, the method introduced in [31] distributes the role of the PKG among a threshold of siblings, that is, nodes at the same level. But the method stops short of discussing a systematic way of choosing the threshold of nodes to act as the PKG. Considering security conditions and energy states of node, Yu *et al*. [49] proposed a revised version of Gennaro *et al*.'s scheme with selection of the best nodes to be used as PGKs from all available ones.

The protocols above are indeed well motivated in terms of their applicability in hierarchical MANETs and are secure against the corruption of any leaves. Unfortunately, their schemes are not designed against the corruption of the nodes of the higher levels in the hierarchy. Guo *et al*. [32] present an efficient hierarchical non-interactive identity-based key agreement protocol based on the pairing cryptography, and it satisfies the desired properties mentioned in [31]. It can resist against any corrupted nodes in the entire hierarchy not only in low levels. Moreover, their scheme captures the dynamic property as in Gennaro *et al*.'s scheme, i.e., nodes can be added to the hierarchy without requiring any further coordination with other nodes and without changing the information held by other nodes. What's more, this scheme isn't based on a threshold-based hierarchical scheme. So, it does not need to set any threshold value. This paper describes algorithms for Setup, Key generation, and Key agreement.

Setup: The key agreement scheme root chooses a set of information for the scheme, such as the maximal depth L of the hierarchy, number of nodes, security parameters, cryptographic functions, domain of keys, etc. It also randomly selects master secret keys $(SK_1, \ldots, SK_L)$ and computes the corresponding public keys $(SK_1 \cdot P_0, ..., SK_L \cdot P_0)$ for a PKG.

Key generation: Given the identity tuple $(ID_1, \ldots, ID_k)$ of node A at level k, PKG can compute A's private key $sk_A = (SK_1 \cdot P_1, ..., SK_k \cdot P_k, SK_{k+1}, ..., SK_L)$, where $P_i = H_1(ID_i)$ $(i=1,...,k)$, and send it to A via an authenticates and private channel. Indeed, node A's parent C with the identity tuple $(ID_1, \ldots, ID_{k-1})$ can compute the private key sk_A using his own private key $sk_C = (SK_1 \cdot P_1, ..., SK_{k-1} \cdot P_{k-1}, SK_k, ..., SK_L)$.

Key agreement: Suppose node A and node B with the identity $(ID_1', \ldots, ID_n')$ ($n<k$) want to establish a shared session secret key, A computes $k_{AB} = e(SK_1 \cdot P_1, P_1')...\cdot e(SK_n \cdot P_n, P_n') \cdot e(SK_{n+1} \cdot P_{n+1}, P_{n+1}')...\cdot e(SK_k \cdot P_k, P_n')$, where $P_j' = H_1(ID_j')$ (j=1,…,n), and B computes $k_{BA} = e(P_1, SK_1 \cdot P_1')...\cdot e(P_n, SK_n \cdot P_n') \cdot e(P_{n+1}, P_n')^{SK_{n+1}}...\cdot e(P_k, P_n')^{SK_{k+1}}$. Obviously, k_{AB} is equal to k_{BA}.

Compared with the other existing schemes, this scheme offers much better performance on the bandwidth consumption, the computational cost, and the storage cost in the case where depth L is relatively small. However, once anyone of node A's ancestor nodes is compromised, the private key of A will be constructed. We will refer to this property as "Ancestors' security matters". Yet it is still an open problem to design an efficient key agreement scheme for a hierarchical MANETs with a large depth.

Tseng *et al*. [33] present the design of Halo, a hierarchical identity-based public key infrastructure that uses hierarchical identity-based cryptography, verifiable secret sharing [24] and threshold/joint secret sharing. Halo was designed to overcome two well-known hurdles: "Absence of Server infrastructure" and "Demand for Opportunistic Collaboration".

In their scheme, each entity (except the leaf node) will choose a secret of their own, and use it to generate the private key of its descendant at the next level. To avoid malicious PKG, they distribute this key among multiple PKGs using the threshold Shamir's secret sharing cryptography [18] to disperse the risks. It extends Shamir's secret sharing scheme by obtaining the secret shares from the additions of contributions from multiple polynomials as we described in [20], [21]. What's more, after categorizing authorities into different cohorts according to their hashed ID value, it will be able to add up shares from different level but same cohort, and recover the secret using polynomial interpolation.

This HIBE contains five algorithms, that is, Root Setup, Lower-Level Setup, Extract, Encrypt and Decrypt.

Root Setup is similar to the master key generation of [20], [21]. After Root Setup, multiple root authorities decide the secret sharing function f(x) with $f(0)=SK_0$, secret share $f(c_i)$ of its cohort c_i, and corresponding qualified set Q-value (Q_0).

Lower-Level Setup: Lower-level PKG (level i) decides the secret sharing function $f_{ski}(x)$, the level secret key sk_i and Q-value Q_i.

Private Key Extraction: PKGs (level k−1) of specific cohort c_i with identity tuple $(ID_1, \ldots, ID_{k-1})$ can generate a partial private key to its predecessor of next level (level k) with identity tuple $(ID_1, \ldots, ID_k)$. PKGs

computes $P_k = H_1(ID_1,...,ID_k)$ and $sk_{k(c_i)} = sk_{k-1(c_i)} + SK_{k-1(c_i)} \cdot P_k$. The PKGs securely transfer $sk_{k(ci)}$ to the entity that asked for a private key. By fetching the threshold t_{k-1} number of $sk_{k(ci)}$, the entity can recover its private key sk_k.

It also discusses the cryptographic mechanisms provided by Halo including the identity-based encryption (HIBE), signature (HIBS) and signcryption (HIBES) operations.

In [32], any node (except leaf node) can obtain the private keys of its children nodes and the root keeps the master secret keys, so the key escrow isn't weakened. In scheme of [33] and polynomial scheme of [31], the PKG at each level (i) is distributed to a threshold (t_i) of siblings, thus the DRKE is $\sum_{i=1}^{L-1} t_i$.

IV. Discussion and Comments

Table I gives an overview of the characteristics of key management of identity-based schemes we mainly introduced above. And the capabilities of keys (the master key pair and private key) generation and distribution are summarized in Table II.

As we can see in Table I, IBC for MANETs is often combined with threshold cryptography to eliminate single-point of failure and resists compromise or insider attack by distributing the PKG service to multiple nodes. Furthermore, with the (t, n) threshold cryptography, honest parties need only contact any t nodes for purpose of obtaining their own key, thus making the protocol resilient to temporary loss of connectivity with other nodes in the network. Secure key generation and distribution are not trivial and required in key management. To improve safety of key generation and distribution, many techniques, such as master key generation in a distributed manner, key proxy, share refreshing, and VSS are proposed to combine with the traditional threshold identity-based mechanism, which is showed in Table II.

TABLE I. Summary of Identity-Based Key Management Schemes

Schemes	Focus on/ main features	DRKE	Key update	Key agreement	Weaknesses
[13]	combine identity-based and threshold cryptography to secure key distribution	t	×	×	Details of key generation not given, need secure channels, Mobile attacks
[20],[21]	detailed implementation of [13]	t	√	√	Mobile attacks
[26]	share refreshing, multicast protocol and key proxy	t	√	√	Require offline TA in the initial stage
[23]	secret share act as private key, standard discrete logarithm assumptions	×	×	√	Single point of failure of online TA
[28],[29]	combination of IBC and the certificateless cryptosystems	√	×	×	Require offline TA in initial stage
[30]	combine certificateless and threshold cryptosystem	√	√	√	Require offline TA in initial stage, details of share transmission not given
[31]	linear hierarchical schemes and non-interactive identity-based key-agreement	$\sum_{i=1}^{L-1} t_i$	×	√	Not against the corruption of the nodes of higher levels, mobile attacks
[32]	resist against any corrupted nodes in the entire hierarchy	×	×	√	Ancestors' security matters, not efficient with a large depth, mobile attacks
[33]	hierarchical ID-based, VSS and threshold cryptography	$\sum_{i=1}^{L-1} t_i$	×	×	Mobile attacks

TABLE II. Summary of Keys Generation and Disteibution

Schemes	TA	Master key pair generated by	PKG	Share of private key transmission	Share update
[13]	No	the initial nodes in a distributed manner	Fully distributed	Secure channel	No
[20],[21]	No	the initial nodes in a distributed manner	Fully distributed	Encrypted by temporary public key	No
[26]	offline	TA	Multicast group and key proxy, partially distributed	Signcryption and multicast, verification of malicious PKG	Yes
[23]	online	TA	TA acts as PKG	VSS validate the correctness	No
[28],[29]	offline	TA	Key combiner, cover all over the network for high level security	Public channel	No
[30]	offline	TA	D-PKGs/D-KGCs	Not mentioned	No
[31]	the root	the root	A threshold of siblings	Not mentioned	No
[32]	the root	the root	Parent node acts as PKG	An authenticated and private channel	No
[33]	No	the initial nodes in a distributed manner	Nodes from different level but same cohort	Not mentioned	No

Threshold identity-based schemes weaken the key escrow problem of PKG (up to the threshold *t*). In certificateless schemes, the private key of node is comprised of two parts, and the PKG does not have access to the user's own secret private key, so certificateless schemes completely address key escrow. What's more, even if adversaries have the entire network lifetime to mount mobile attacks and they compromise or disrupt enough PKGs, a threshold identity-based scheme using certificateless cryptography can prevent adversaries to derive the private keys of nodes from the compromised PKGs. Thus, this scheme also resists against mobile attacks.

A MANET is usually assumed to be homogeneous, where each mobile node shares the same radio capacity. However, a homogeneous ad hoc network often suffers from poor scalability. Ref. [50] observed that, when using the same amount of sensor nodes in a given coverage area for flat and hierarchical topologies, that the system throughput capacity increases, while system delay decreases. Ref. [51] showed that a hierarchical key management scheme is a very promising way to achieve good scalability. Meanwhile, the hierarchy of PKG service nodes reduces normal nodes' exposure to the compromised PKG nodes, thus hierarchical identity-based schemes weaken the key escrow problem. By the way, there are some other techniques we don't introduce to eliminate or weaken key escrow of IBC, such as, certificate-based cryptosystem [52], reducing the trust of PKG [53].

There are two points that needs to be noted in identity-based schemes for MANETs. First, in threshold-based schemes, the threshold parameter *t* controls the trade-off between security and service availability. Choosing a value of 1 for *t* causes the least security while keeping highest service avail ability. On the other hand, selecting a value of *n* for *t* results a maximum security but weak service availability. Second, the new node can only contact its 1-hop neighbors, and if no enough nodes are in proximity then it cannot obtain a key. Deng *et al*. suggest that the node moves in order to find a sufficient number of PKGs. More seriously, nodes have to trust their 1-hop away neighbors to route all information. It makes scheme more vulnerable to Sybil attacks [54], in which a single node presents multiple identities to others. But this problem can be addressed by periodically refreshing the master key, and introducing a trust management technique [55] and an Intrusion Detection System.

A. Techniques to Improve Identity-Based Scheme

Key management is an important part of secure communication that is responsible for secure key generation, key distribution and key maintenance. Here are techniques in the literature to improve security and availability of key management of identity-based scheme for MANETs.

- Improved threshold cryptography for key generation and distribution: The master key pair is generated by the initial nodes in a distributed manner, and there is no need of TA to distribute secrets of master private key to nodes. To counter mobile attacks, we suggest secret refreshing mechanism in which secret shares are updated in intervals and new shares cannot be combined with old ones to recover the secret. To secure the share of private key transmission, we can employ VSS to verify integrity of secret shares of threshold cryptography.
- Certificateless cryptography to eliminate key escrow: Certificateless cryptography completely addresses the key escrow problem and mobile attacks by having the user contribute to the private key generation.
- Hierarchical for special MANETs: We can take the hierarchical cryptography into consideration if the organization of the network is hierarchical in nature or the network requires good scalability.

V. Conclusions

Several cryptographic mechanisms for secure MANETs can be found in the literature. Among them, identity-based cryptography, a special form of public key cryptography, is more suitable for bandwidth-limited and resource-constrained MANETs, because it eliminates the requirement for a certificate authority and public key certificates. In this survey paper, we have divided identity-based key management schemes for MANETs into four types: traditional threshold identity-based schemes, SSPK identity-based schemes, certificateless schemes, and hierarchical identity-based schemes. Then we have studied one or more typical schemes for each type, and discussed their approaches, strengths, and weaknesses. Last, we have made a summary of their key management and keys generation and distribution, and pointed out the trade-off problem of threshold parameter *t* and 1-hop-trust problem. During the survey, we also suggest some techniques to improve the security of key management of identity-based scheme for MANET. How to combine those effective security techniques to secure the key management is one of our future works.

We have mentioned many properties of IBC that make it especially attractive for MANETs. However, there are still some problems not completely addressed and impedes application of IBC, *e.g*. identity disclosure, key revocation, high computations in elliptic-curve. We will try to explore deeper in these research areas.

References

[1] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks in mobile ad hoc networks," in *Proc. 25th IEEE Canadian Conference on Electrical and Computer Engineering*, 2012, pp. 1-6.

[2] A. L. S. Orozco, J. G. Matesanz, L. J. G. Villalba, J. D. M. D áz, and T.-H. Kim, "Security issues in mobile ad hoc networks" *International Journal of Distributed Sensor Networks*, vol. 2012, Dec 2012.

[3] P. M. Jawandhiya, M. M. Ghonge, M. S. Ali, and J. S. Deshpandee, "A survey of mobile ad hoc network attacks,"

International Journal of Engineering Science and Technology, vol. 2, no. 9, pp. 4063-4071, 2010.

[4] *Handbook of Applied Cryptography*, A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, CRC press, 2010.

[5] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 380-400, May 2012.

[6] T. Bhatia and A. K. Verma, "Security issues in manet: A survey on attacks and defense mechanisms," *International Journal Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 1382-1394, Jun 2013.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Adv. Cryptology—CRYPTO*, vol. 2139, New York, 2001, pp. 213-229.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO 84 on Adv. in Cryptology*, New York, 1985, pp. 47-53.

[9] B. Waters, *Efficient Identity-based Encryption Without Random Oracles*, Aarhus, Denmark: Springer-Verlag, 2005, pp. 114-127.

[10] J. C. Cha and J. H. Cheon, *An identity-based Signature From Gap Diffie-Hellman Group*s, FL, USA: Springer-Verlag, 2002, pp. 18-30.

[11] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proc. 9th Annual International Workshop on Selected Areas in Cryptography*, Newfoundland, 2002, pp. 310-324.

[12] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Proc. International Conf. on the Theory and Applications of Cryptographic Techniques*, Interlaken, 2004, pp. 223-238.

[13] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proc. Symp. on Applications and the Internet Workshops*, 2003, pp. 342-346.

[14] D. Boneh, B. Lynn, and H. Shacham, *Short Signatures From the Weil Pairing*, Gold Coast, Australia: Springer -Verlag, 2001, pp. 514-532.

[15] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. 10th Annual Conf. for Australian Unix User's Group*, 2004, pp. 95-102.

[16] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Proc. Cryptology—CRYPTO'89*, New York, 1990, pp. 307-315.

[17] Y. G. Desmedt, "Threshold cryptography," *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 449-458, July/Aug 1994.

[18] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov 1979.

[19] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24-30, Nov/Dec 1999.

[20] H. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks," in *Proc. International Conf. on Information Technology: Coding and Computing*, vol. 1, 2004, pp. 107-111.

[21] H. Deng and D. P. Agrawal, "TIDS: Threshold and identity-based security scheme for wireless ad hoc networks," *Ad Hoc Networks*, vol. 2, no. 3, pp. 291-307, July 2004.

[22] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Proc. Cryptology—EUROCRYPT*, Brighton, 1991, pp. 522-526.

[23] N. Saxena, "Public key cryptography sans certificates in ad hoc networks," in *Proc. 4th International Conf. on Applied Cryptography and Network Security*, Singapore, 2006, pp. 375-389.

[24] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing,' in *Proc. 28th Annual IEEE Symposium on Foundations of Computer Science*, Los Angeles, 1987, pp. 427-438.

[25] S. Zhao and A. Aggarwal, "Against mobile attacks in mobile ad-hoc networks," in *Proc. International Conf. on Information Theory and Information Security*, Beijing, 2010, pp. 499-502.

[26] G. Li and W. Han, *A New Scheme for Key Management in Ad Hoc Networks*, Reunion Island, France: Springer-Verlag, 2005, pp. 242-249.

[27] S. S. Al-Riyami and K. G. Paterson, *Certificateless Public Key Cryptography*, Taipei, Taiwan: Springer-Verlag, 2003, pp. 452-473.

[28] X. Lv, H. Li, and B. Wang, "Identity-based key distribution for mobile ad hoc networks," *Frontiers of Computer Science in China*, vol. 5, no. 4, pp. 442-447, Dec 2011.

[29] X. Lv, H. Li, and B. Wang, "Virtual private key generator based escrow‐free certificateless public key cryptosystem for mobile ad hoc networks," *Security and Communication Networks*, vol. 6, no. 1, pp. 49-57, Jan 2013.

[30] L. Li, Z. Wang, W. Liu, and Y. Wang, "A certificateless key management scheme in mobile ad hoc networks," in *Proc. 7th International Conf. on Wireless Communications, Networking and Mobile Computing*, Wuhan, 2011, pp. 1-4.

[31] R. Gennaro, S. Halevi, H. Krawczyk, T. Rabin, S. Reidt, and S. D. Wolthusen, *Strongly-resilient and Non-interactive Hierarchical Key-agreement in MANETs*, Málaga, Spain: Springer Berlin Heidelberg, 2008, pp. 49-65.

[32] H. Guo, Y. Mu, Z. Li, and X. Zhang, "An efficient and non-interactive hierarchical key agreement protocol," *Computers & Security*, vol. 30, no. 1, pp. 28-34, Jan 2011.

[33] F. K. Tseng, J. K. Zao, Y. H. Liu, and F. P. Kuo, "Halo: A hierarchical identity-based public key infrastructure for peer-to-peer opportunistic collaboration," in *Proc. 10th International Conf. on Mobile Data Management: Systems, Services and Middleware*, Taipei, 2009, pp. 672-679.

[34] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "AC-PKI: Anonymous and certificateless public-key infrastructure for mobile ad hoc networks," in *Proc. International Conf. on Communications*, vol. 5, 2005, pp. 3515-3519.

[35] H. Sun, X. Zheng, and Z. Deng, "An identity-based and threshold key management scheme for ad hoc networks," in *Proc. International Conf. on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, vol. 2, 2009, pp. 520-523.

[36] Z. Ping, R. Hu, Y. Fang, and J. Yang, "A key management scheme for ad hoc networks," in *Proc. 5th International Conf. on Wireless Communications, Networking and Mobile Computing*, Beijing, 2009, pp. 1-5.

[37] K. G. Paterson, "ID-based signatures from pairings on elliptic curves," *Electronics Letters*, vol. 38, no. 18, pp. 1025-1026, Aug 2002.

[38] B. Lynn, "Authenticated identity-based encryption," IACR Cryptology ePrint Archive, Report 2002/072, July 2002.

[39] R. Hauser, T. Przygienda, and G. Tsudik, "Reducing the cost of security in link-state routing," in *Proc. Symposium on Network and Distributed System Security*, San Diego, 1997, pp. 93-99.

[40] X. Boyen, *Multipurpose Identity-based Signcryption*, California, USA: Springer-Verlag, 2003, pp. 383-399.

[41] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proc. CRYPTO 84 on Advances in Cryptology*, 1985, pp. 10-18.

[42] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of cryptology*, vol. 4, no. 3, pp. 161-174, Jan 1991.

[43] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388-404, Mar 2000.

[44] D. L. Gu, G. Pei, H. Ly, and M. Gerla, "Hierarchical routing for multi-layer ad-hoc wireless networks with UAVs," in *Proc. 21st*

Century Military Communications Conf., Los Angeles, 2000, pp. 310-314.
[45] S. Zhao, K. Tepe, I. Seskar, and D. Raychaudhuri, "Routing protocols for self-organizing hierarchical ad-hoc wireless networks," in *Proc. IEEE Sarnoff Symposium*, 2003.
[46] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Proc. International Conf. on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, Amsterdam, 2002, pp. 466-481.
[47] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Proc. 12th Annu. International Cryptology Conf. on Advances in cryptology*, Santa Barbara, 1993, pp. 471-486.
[48] M. Ramkumar, N. Memon, and R. Simha, "A hierarchical key pre-distribution scheme," in *Proc. IEEE International Conf. on Electro Information Technology*, Lincoln, 2005, pp. 6.
[49] F. R. Yu, H. Tang, P. C. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Transactions on Network and Service Management*, vol. 7, no. 4, pp. 258-267, Dec 2010.
[50] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139-172, 2001.
[51] K. Xu, X. Hong, and M. Gerla, "An ad hoc network with mobile backbones," in *Proc.IEEE International Conf. on Communications*, 2002, pp. 3138-3143.
[52] Z. Li, X. Xu, and C. Li, "Provably secure certificate-based signature scheme for ad hoc networks," *Journal of Networks*, vol. 7, no. 11, pp. 1845-1851, Nov 2012.
[53] V. Goyal, *Reducing Trust in the PKG in Identity based Cryptosystems*, Santa Barbara, USA: Springer-Verlag, 2007, pp. 430-447.
[54] S. Abbas and M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in MANETs," *System Journal*, vol. 7, no. 2, Jun 2013.
[55] T. Moore, J. Clulow, S. Nagaraja, and R. Anderson, *New Strategies for Revocation in ad-hoc Networks*, Cambridge, UK: Springer-Verlag, 2007, pp. 232-246.

Kuo Zhao received the B.E degree in Computer Software in 2001 form Jilin University, followed by M.S degree in Computer Architecture in 2004 and Ph.D. in Computer Software and Theory from the same university in 2008. He is currently Senior Lecturer in the College of Computer Science and Technology, Jilin University. His research interests are in identity-based cryptography, computer networks and information security.

Longhe Huang was born in Jiangxi, China in 1989. He received the B.S. degree from the College of Computer Science and Technology, Jilin University, Changchun in 2012, and he is currently working toward the M.S. degree at Jilin University. His research interest includes identity-based cryptography, and the security of wireless network.

Fangming Wu received his B.S. degree from the PLA Information Engineering University in 2007. He is currently pursuing in the College of Computer Science and Technology, Jilin University. His research interest is the communication of WSN, computer networks and information security.

Liang Hu Dr Liang Hu had his BEng on Computer Systems Organization in 1993 and his PhD on Computer Software and Theory in 1999. He is currently Professor and PhD supervisor of College of Computer Science and Technology, Jilin University, China.
His main research interest includes network security and distributed computing, including related theories, models, and algorithms of PKI/IBE, and IDS/IPS.
As a person in charge or a principal participant, Dr Liang Hu has finished more than 20 national, provincial and ministerial level research projects of China.