Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Security in Mobile Ad-Hoc Networks using Cryptography

[1]Shalini Saini, [2]Asst. Professor Abhishek Shukla, [3]Dr. Manish Verma
[12]Uttar Pardesh Technical University Lucknow, India
[3]R.D. Engineering College Technical Campus, Ghaziabad, Uttar Pardesh, India

Abstract— Security in mobile ad-hoc networks (MANETs) continues to attract attention after years of research. Recent advances in identity-based cryptography (IBC) sheds light on this problem and has become popular as a solution base. We present a comprehensive picture and capture the state of the art of IBC security applications in MANETs based on a survey of publications on this topic since the emergence of IBC in 2001. In this paper, we also share insights into open research problems and point out interesting future directions in this area.

Index Terms—Identity-based Cryptography, Mobile Ad-hoc Networks

I. INTRODUCTION

Research on security of MANETs remains active, in spite of years of exploration, in both academia and industry. It is partially due to the fact that no mature solution is widely accepted and the growing availability of small, personalized mobile devices with peer to peer communication capability through wireless channels.

General security requirements for MANETs include [1]: Data Confidentiality that keeps data secret to outsiders, Data Integrity that prevents data from being altered, Data Freshness that keeps data in the correct order and up-to-date, Data Availability that ensures data to be available on request, Data & Identity Authentication that verifies that the data or request came from a specific, valid sender, and Non-repudiation that ensures a node cannot deny sending a message.

Security mechanisms that are widely used and proven to be effective in wired networks are not always applicable to MANETs. Attacks that can be effectively detected and prevented in wired networks have been big security challenges in MANETs. Examples include, but are not limited to, iden-tity/address spoofing, message tampering and forgery, message replay, etc. Compared to wired networks, the combination of the following characteristics of MANETs make it especially difficult to achieve security requirements:

- Lack of a network infrastructure and online administra-tion.
- Network topology and node membership dynamics.
- The potential insider attacks.

Security proposals in early research are typically attack-oriented. They often first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart them. Such solutions are designed explicitly against limited attack models. They work well in the presence of

limited attack models., but may collapse under combined or unanticipated attacks [2].

Cryptography is then used to provide a general design framework. Cryptography techniques used in MANETs can be classified into two categories, namely, *Symmetric Key based* and *Asymmetric Key based*. In symmetric key based schemes, if an attacker compromises the symmetric key of a group of users, then all encrypted messages for that group will be exposed. Asymmetric key based schemes can provide more functionalities than symmetric ones, e.g., key distribution is much easier, authentication and non-repudiation are available, compromise of a private key of a user does not reveal messages encrypted for other users in the group. However, they are generally computationally expensive.

Traditional asymmetric cryptography widely and effectively used in the Internet relies on a Public Key Infrastructure (PKI). The success of PKI depends on the availability and security of a Certificate Authority (CA), a central control point that everyone trusts. In general MANETs, applying PKIs by maintaining a central control point is clearly not always feasible. Another obstacle that impedes PKI's employment in MANETs is the heavy overhead of transmission and storage of public key certificates (PKCs).

Identity-based cryptography (IBC) is a special form of public key cryptography. It is an approach to eliminate the requirement of a CA and PKCs. Since 2001, IBC has attracted more and more attention from security researchers. Some properties of IBC make it especially suitable for MANETs. Fang et al. [3], [4] summarize the advantages of IBC to MANETs:

- Easier to deploy without any infrastructure requirement. This saves certificate distribution, while bringing "free" pairwise keys without any interaction between nodes.
- Its resource requirements, regarding process power, stor-age space, communication bandwidth, are much lower.
- The public key of IBC is self-proving and can carry much useful information.

We believe that IBC, with its fast development in recent years, is a promising solution for MANET security issues. This has motivated us to write this survey. We present a comprehensive picture and have identified the state of the art of important IBC

security applications in MANETs by conducting a survey on publications over the recent decade from 2001 to 2010. We also share insights into open research problems and point out interesting future directions in this area. Since diffic ulty of MANET security lies on differences between MANETs and wired infrastructured networks in network and lower layers, identity-based cryptosystems are mostly employed in network layer, i.e. in routing protocols. Hence, most of previous publications, and we, focus on key management and routing protocols. A non-trivial point of this survey is that we review the proposals in the literature from a system engineering perspective as to how a practical system works with these existing proposals, e.g., how to set up a secure routing among a set of nodes. In this perspective, we identify some weaknesses of these protocols which cannot be found if we look at them separately.

The survey is organized as follows: Section II briefly reviews the background of research on security of MANETs and IBC, and summarizes important publications in the development of IBC which have had a great influence on security of MANETs. Sections III to V review and summarize schemes applying IBC to MANETs, in sub-areas of key management, secure routing, and other applications. Section VI presents some remaining issues and potential research directions of applying IBC to MANETs. Section VII identifies the suitable market of IBC in MANETs and concludes the survey.

II. BACKGROUND

A. 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 IBC was first proposed by Shamir [5] in 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 a 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.

For a long time after Shamir published his idea, the development on IBC was very slow. Joux [6], 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 agreement. This was one of the breakthroughs in key agreement protocols. After this, Boneh and Franklin [7] presented at 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.

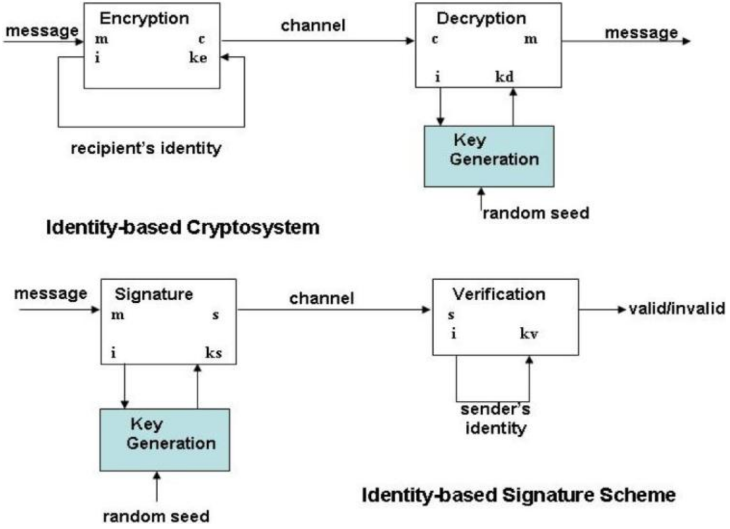

Fig.1:shamir’s identity based cryptosystem and signature scheme

B. Preliminaries of Identity-based Cryptography

Unless otherwise stated, in this and following sections we use the same notations as in this section, which are summarized in Table I.

In [5], Shamir introduced a novel type of cryptographic scheme, the 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.

Figure 1 illustrates his idea: In an identity-based cryptosystem, the recipient’s identity i is used to generate the encryption key, and the decryption key is derived from i and a random seed k. In an identity-based signature scheme, the signature key is generated from sender identity i and a random seed k, and the verification key is derived from sender’s from sender identity i and a random seed k, and the verification key is derived implementation principals:

- 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
- 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 the RSA scheme is not capable for his scheme.

The most frequently used assumptions are [09, pp. 7]:

- **Computational Diffie-Hellman (CDH) problem in** H_1: there is no efficient algorithm to compute $m\hat{}(R,R)^{cd}$ from $R, cR, dR \in H_1$ for $c, d \in W^*_q$.
- **Weak Diffie-Hellman (W-DH) problem in** H_1: there is no efficient algorithm to compute rT from $R, T, rR \in H_1$ and $r \in W^*_q$. (W-DH problem is no harder than CDH problem).
- **Bilinear Diffie-Hellman (BDH) problem in** $(H_1, H_2, m\hat{})$: there is no efficient algorithm to compute $m\hat{}(R,R)^{cdf} \in H_2$ from $R, cR, dR, fR \in H_1$ where $c, d, f \in . W^*_q$
- **Decisional Bilinear Diffie-Hellman (DBDH) problem in** $(H_1, H_2, m\hat{})$: there is no efficient algorithm to decide if $u = m\hat{}(R,R)^{cdf}$ given $u \in H_2$ and c,d,f $\in . W_q^*$.

A *Symmetric Bilinear Map* is denoted $m\hat{} : H_1 \times H_1 \rightarrow H_2$ between two cyclic groups H_1, H_2 of order q for some large prime q,

where H_1 is the group of points of an elliptic curve over M_e and H_2 is a subgroup of $M^*_e{}^2$.

A cryptographic bilinear map satisfies the following properties [9, pp. 6]:

1) **Bilinear**: $m\hat{}(cR, dT) = m\hat{}(R, T)^{cd}$ for all $R, T \in H_1$ and all $c, d \in W^*_q$. This can be restated in the following way. For $R, T, Y \in H_1$, $m\hat{}(R + T, Y) = m\hat{}(R, Y)\, m^{\wedge}(T, Y)$ and $m\hat{}(R, T + Y) = m\hat{}(R, T) m^{\wedge}(R, Y)$.
2) **Non-degenerate**: $m\hat{}(R, R) \in M^*_{e2}$ is an element of order q, and in fact a generator of H_2. In other words, $m\hat{}(R, R) \neq 1$
3) **Computable**: Given $R, T \in H_1$ there is an efficient algorithm to compute $m\hat{}(R, T)$.

Their scheme is specified by four randomized algorithms [7, pp. 215]:

- Setup: The algorithm maps arbitrary string identities to points on an elliptic curve. Set the system public key R_{pub} as rR where a is a random number in W^*_q, and R is an arbitrary point in Q/M_e of order q. Choose a cryptographic hash function $L : M_e^2 \rightarrow \{0, 1\}^h$ for some h. Choose a cryptographic hash function $K : \{0, 1\}^h \rightarrow M_e$. The system parameters are $params = \{x, h, R, R_{pub}, K, L\}$. The master-key is $z \in W_q$.

Table I: Notations Used In This Survey

Symbols	*meanings*
$L(i)$	a hash function
W	set of integers
Wn	set of integers mod n
Mq	the finite field with q elements
W^*_q	the multiplicative group of integers modulo prime number q. $Z^*_q = \{a \mid 1 \leq a \leq q - 1\}$
Q/M_e	elliptic curve over M_e
m : H1 × H1 → H2	a bilinear map between two cyclic groups H1,H2
R	an arbitrary point in Q/M_e
t_{UV}	private key of UV
T_{UV}	private key of UV
Z	master secret key
Rpub	system public key

- Extract: For a given string $UV \in \{0, 1\}^h$, the algorithm builds public key for UV: $T_{UV} = K(UV)$, a point in Q/M_e mapped from UV, and the private key t_{UV} as $T_{UV} = Zt_{UV}$.
- Encrypt: Choose a random $a \in W_q$, and set the ci-phertext to be B= $\{aR, N \oplus L(s_{UV}{}^a)\}$ where $s_{UV} = m\hat{}(T_{UV}, R_{pub}) \in M_e2$
- Decrypt: Let $B = \{X, E\}$ be a ciphertext encrypted using the public key of UV, decrypt C using the private key $T_{UV} : E \oplus L(e\hat{}(t_{UV}, X)) = N$

C. Threshold Cryptography and Key Management *in MANETs*

Many IBC schemes use threshold cryptography which originated from Shamir [10], for their key management. Shamir gives a solution to the problem of sharing a secret among a number of users in [10]. In his paper, he identifies the problem of how to divide data A into o pieces in such a way that A is easily reconstructable from any p pieces, but even complete knowledge of $p - 1$ pieces reveals absolutely no information about A.

Shamir proposes a (p, o) threshold scheme to solve this problem based on polynomial interpolation: given p points in the dimensional plane $(a_1, b_1) \ldots (a_t, b_t)$, with distinct a_i'o, there is one and only one polynomial $f(y)$ of degree $p - 1$ such that $f(y) = b_i$ for all i. To divide the secret A into p pieces, he suggests picking a random $p - 1$ degree polynomial $f(y) = b_0$

+ $b_1x + \cdots + b_ta^{p-1}$ in which $b_0 = A$, and each piece is the value of the polynomial at the n points: $A_1 = f(1), \ldots, A_i = f(i), \ldots, A_n = f(o)$. Thus any subset of p of the pieces can determine the coefficients of the polynomial (using e.g. Lagrange interpolation) and thus the secret data at a certain point. 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.

III. KEY MANAGEMENT USING IBC

Cryptographic techniques are often at the center of solving security problems in MANETs and hence need key management. Key management in IBC requires key generation and distribution methods, and ideally key protection and revocation. This section reviews and discusses proposals for IBC key management in MANETs.

Master Key and Private Key Generation

Most of the master key and private key generation schemes are derived from and are variants of [7]. The criteria to judge this type of scheme is use of their four primitive algorithms. In this section, we first provide some examples based on traditional threshold cryptography of [34] and discuss the limitations of these schemes, and then discuss some proposals that attempt to improve traditional threshold cryptography. We give some key generation schemes tweaked for specific purposes: e.g. high privacy, compromise-tolerance, or light-weight.

Key Generation Using Traditional Threshold Cryptography:

PKG plays a fundamental role in an identity-based cryptosystem, but it is not trivial to have a robust PKG in a MANET environment. As Zhou et al. have suggested [34], a CA service of PKI can be distributed to multiple nodes in a MANET environment. This idea is also applicable to IBC.

Khalili et al. [11] propose to use IBC to secure ad hoc networks. The authors refer to the work of [34], [12] and identify the problem that all proposed key management solutions assume either pre-existing shared secrets among nodes or the presence of a common PKI. They 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 identities as their public keys. The secret key, corresponding to the public key, is computed by having the node obtain t shares of their key from 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 [7].

As a detailed implementation of Khalili's idea, Deng et al. [13], [14] propose an identity-based key management and authentication system for MANET, using 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 distributed way. The author implemented a scheme with distributed master key generation,private key generation,secret share update, and secret share generation for a new joining node.

Xia's scheme [15] is also very similar to Deng's scheme: A set of Distributed PKG nodes collaboratively generate system public key and master key in a fully distributed manner; Shares can be updated among PKGs; New nodes can get their shares from PKGs and become new PKG nodes.

Differences from Deng's scheme are:

1) This scheme does not use temporary PKI for secret share distribution as in Deng's scheme. Instead, it employs a self-generated public/private key pair in the following way: each DPKG node computes a temporary public key and sends it to other DPKG nodes. Secret shares are encrypted and decrypted using this temporary public key.
2) The paper applies their scheme in OLSR routing protocol, particularly use HELLO messages and TC messages in OLSR to select and mark DPKG nodes, while Deng et al. apply their scheme in DSR routing protocol.

These differences lead to the following problems:

1) Each DPKG node has to store in memory the temporary public keys of other DPKG nodes.
2) System public key and master key collection process is not secure, because only public channels are available at this stage.
3) The keys generated are not guaranteed secure, because it does not provide any security protection for OLSR routing protocol it relies on.

All of these schemes use threshold cryptography to distribute the functionality of PKG to multiple nodes. Due to threshold cryptography, these schemes have the following weaknesses:

1) Interdependency Cycle between Secure Routing and Security Services: These scheme rely on some existing routing or online administration mechanisms (e.g. out-of-band communicant, side channel) to distribute secret shares among the distributed PKG nodes. Thus, they cannot be used in secure routing protocols that would require secure keys. This is noted as the problem of interdependency cycle between security services and secure routing [16], [17].

2) Proximity-caused Insecurity: In some circumstances where a node can move in order to access to more nodes, one way to avoid the routing-security interdependency cycle problem is to have a threshold number of authorized users that are physically close to each other (i.e., within one-hop communication distance so that routing is eased). This incurs another related problem—the proximity-caused insecurity: it is possible that an adversary compromises these nodes within a short period of time (e.g., by capturing the nodes and/or compromising them one by one) [17]. Furthermore, the proximity-based solution is not applicable to fully distributed key generation schemes where all nodes participate in and contribute to the key generation, and thus routing connecting all nodes (not only among a threshold number of nodes) is still required.
3) Mobile Attacks: Threshold cryptography is subject to mobile attacks, in which a mobile adversary could move to compromise multiple nodes and reveal the secret shares of them in order to recover the secret. To counter mobile attacks, the above proposals use secret refreshing mechanism in which secret shares are updated in intervals and new shares cannot be combined with old ones to recover the secret. They assume a mobile adversary cannot compromise enough authentic nodes within the share refreshing period. Merwe et al. in [16] do not think this assumption is practical. We have a separate paper analyzing this issue and proposing solutions [18].

IV. SECURE ROUTING PROTOCOLS USING IBC

Routing in MANETs enables packet delivery from one node to another by way of intermediate nodes. It is the fundamental issue considered in MANETs, thus secure routing is a fundamental issue in MANET security. Secure routing ensures successful routing among authentic nodes with adversary nodes existing around or inside the network, and forms the bedrock of a secure MANET system. An important application of IBC in MANETs is to design secure routing protocols. Generally, compared to traditonal cryptosystems, IBC provides the following advantages in terms of secure routing:

- IBC improves efficiency of secure routing. Once secure keys are avaiable, IBC can be applied to either on-demand routing protocols like DSR, or link state routing protocols like OLSR. The routing messages encrypted and signed by the sender and decrypted and verified by the receiver using IBC. To protect routing messages, on same security level, IBC encryption/decryption schemes are faster, and IBC signature is shorter.

A. A Security Architecture to Secure OLSR

Adjih et al. [21] propose a security architecture to secure OLSR using IBC.

Their proposal is based on the work of [20], [8]. In their scheme, an (offline) TA 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 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.

Technical details of the scheme are not given in the paper, e.g. how keys are generated and distributed, how packets are signed and encrypted.

B. A Key Management Integrated OLSR Routing Protocol

Most routing protocols do not consider key management issues. In [22], Zhao and Aggarwal propose a secure routing protocol integrated with key management. Based on previous work of [7], [23], [19], and using proposed proactive security approach, they design a secure routing protocol for pre-planned MANETs.

The network starts with initial nodes. The first phase is routing setup. Initial nodes contact and get system secret from an off-line official administrator. With the system secret, the nodes communicate with each other securely and set up routing table. The second phase is secret update. Since routing is already set up, initial nodes can communicate with each other securely using pair-wise session key and contribute to a new secret. System secret can be updated periodically or when necessary.

When node *A* sends a routing message, including *HELLO* and *TC* message, it encrypts and authenticates the message as follows:

1) *Encrypting the message:* The entire message, N , is encrypted using a symmetric encryption function S. The symmetric encryption key is calculated as: $p = G_1(f^w)$, where $f = m\hat{}(g_B, Q\ )$, w is a random number in W_q * $(w \cdot T_B \neq \infty)$. f can be stored in the node's memory for future use until secret update. The encrypted message $J_p(N\ )$ is put in the message field.
2) *Signing the message and message header:* A signature is calculated over the message header except the *Time To Live (TTL)* and *Hop Count (HC)* fields, and the

encrypted message. Assume the encrypted message to be signed is N_1, the secret authentication key is calculated as $L_1 = G_2(N_1,f^w)$. The authentication code $\theta = GN\ BD(L_1,N_1)$ and $w \cdot Q_A$ are appended at the end of the message.

OLSR packet is also signed and encrypted, and verified at each hop with *TTL* and *HC* fields recalculated. Authentic intermediate nodes and destination node can decrypt and verify the packets by computing the key $\mathrm{g}^{\mathrm{w}} = m\hat{}(T_B, R_{pub})^w = m\hat{}(w \cdot T_B, R_{pub})$, $p = G_1(f^w)$. This scheme addresses routing-security interdependency cycle, by way of secret pre-distribution, which is not a problem in pre-planned, or so-called authority-based, MANETs.

V. APPLICATIONS OF IBC IN SPECIAL-PURPOSE MANETS

Besides key management and secure routing, there are also some other applications of IBC in special MANETs, such as multi-domain or multi-TA coalition networks. These applications are not relevant to general MANETs, thus we deliberately leave out much of the detail in the following.

In [24], Balfe et al. envisage that in IBC infrastructures, entities from multiple TAs might be present within a larger coalition structure, with each TA issuing cryptographic keys to entities in its own security domain. Based on the work of [25], [26], [11], [27], they propose a lightweight, generic and broadly applicable framework enabling the refreshing of privates keys in coalition-forming situations. They point out their contribution is the improvement upon the obvious approach of simply distributing new private keys by encrypting them using the old public keys.

The authors claim that their scheme is secure and state

that the framework is applicable to enable secure inter-operation between entities with different trusted authorities in dynamic coalitions environments, and is particularly well-suited to coalition forming in computation and bandwidth-limited MANETs.

In [28], Li et al. consider cross-domain key agreement in multi-domain ad hoc networks. They propose a new IBC scheme based on multiple PKGs, which is more suitable for multi-domain ad hoc networks. They assume that there are two PKGs—$P\ KG_1$ and $P\ KG_2$ for two domains, which share the same system paremeters, but have different master private keys. In this situation, the scheme provides encryption/decryption, sign/verify functions between the two domains.

Cai et al. [29] apply IBC 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 for MANETs.

The authors design a lightweight and cheat-resistant micro-payment scheme to stimulate and compensate collaborative peers that sacrifice their resources to relay packets for other peers. They base their work on [30], [7]. 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 MANETs; and with profitable collaboration, system utility increases when peers have maximized their potential profit.

In this section, we have studied applications of IBC in special-purpose MANETs. These applications are only applicable to very limited scenarios, and are not popularly useful.

A. Security Concerns of IBC

The greatest concern of applying IBC in MANETs is the reliability of its security. In [31], Granger et al. state that it is still hard to say whether pairing-based cryptosystems (the mainstream of IBC) 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 (bilinear Diffiee-Hellman problem) 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 is a source of concern that security depends on the presumed intractability of the DHP rather than the more natural and more extensively studied Discrete Log Problem (DLP).

Verheul [32] shows an example in which the DHP is efficiently solvable. The author 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. From the literature, it seems that up to now, Verheul's guess has not been proven positive or negative. In a more recent article [33], Moody reviews some of the problems that the security of elliptic curve cryptosystems are based upon, and discusses in detail the theorem of Verheul (including its generalization), and its consequences. The author tries to

generalize Verheul's theorem to more ordinary curves. As a conclusion, the author leaves it as an open question to generalize some form of Verheul's theorem to ordinary curves with low embedding degree, and states that this work would require new methods.

To achive high security and counter attacks towards IBC, researchers suggest putting more strict restraints on its mathe-matical basis and choosing the elliptic curve and finite field it uses meticulously. Researches on these security concerns and challenges will be the future work on IBC schemes and their applications.

VI. CONCLUSIONS

In this survey, we have studied major developments in IBC, and the applications of IBC in MANETs in various areas. We have identified the drawbacks and challenges of IBC which impose difficulties on its application to MANETs.

In the field of MANETs' security IBC has already been widely applied. However, we notice there are many issues unaddressed in these applications.

To apply IBC better in MANETs, we must look at properties of IBC and identify its pros and cons. On the one hand, some properties lend IBC attractions to MANETs: private keys are short and easy to generate and store, public keys are implicitly carried by their identities, so there is no need to distribute and store certificates of partners or public key of

CA. On the other hand, its other properties appear awkward in MANETs,. Another thing that is not mentioned there (because there is no way to work around it) but a problem for many MANETs is that: from the nature of IBC, it requires the system parameters be distributed to all communicating parties before any messages can be en-crypt/decrypted. This requirement excludes the so called "truly ad hoc" networks out of its scope. In those networks, a group of strangers come together without any central node in charge of the administration and the organization of the network. The master key can only be generated online contributively by

untrusted peers. Thus, they are inevitably subject to Byzantine attacks, and may be totally taken over by adversaries.

Considering properties on both sides of IBC in MANETs, we find a type of MANETs that is most suitable for IBC: there is an administrator that generates and distributes initial system parameters to all nodes; the administrator can authenticate the identity of a node, and assign initial private key to it. For those MANETs that meet these requirements, e.g., sensor networks, military networks such as moving soldiers with wearable computers, portable communication systems for future public safety, emergency and disaster applications, IBC is the most promising security solution, but there seem no perfect solutions yet. We suggest future research be focused on this type of MANETs.

REFERENCES

[1] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys & Tutorials, IEEE*, vol. 10, no. 4, pp. 78–93, 2008.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wirel. Commun.*, vol. 11, no. 1, pp. 38–47, 2004.

[3] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *Wireless Commun.*, vol. 16, no. 2, pp. 24–29, 2009.

[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable Secur. Comput.*, vol. 3, no. 4, pp. 386–399, 2006.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Crypto 1984*, 1984.

[6] A. Joux, "A one round protocol for tripartite diffie-hellman," in *ANTS IV*, ser. LNCS, vol. 1838. Springer-Verlag, 2000, pp. 385–394.

[7] Boneh and Franklin, "Identity-based encryption from the weil pairing," in *Proc. Crypto 2001*, ser. LNCS, vol. 2139. Springer, 2001, pp. 213– 219

[8] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. ASIACRYPT*, ser. LNCS, vol. 2248. Springer-Verlag, 2001, pp. 514–532.

[9] R. Dutta, R. Barua, and P. Sarkar, "Pairing-based cryptographic proto-cols: A survey," Cryptology ePrint Archive, Report 2004/064, Jun. 24 2004

[10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, 1979.

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

[12] R. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh, "Bootstrapping security associations for routing in mobile ad-hoc networks," in *IEEE Global Telecommunications Conference 2003*. IEEE Computer Society Press, 2003.

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

[14] 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, 2004.

[15] P. Xia, M. Wu, K. Wang, and X. Chen, "Identity-Based Fully Distributed Certificate Authority in an OLSR MANET," in *4th Wireless Communi-cations, Networking and Mobile Computing*. IEEE, 2008, pp. 1–4.

[16] J. V. D. MERWE, D. DAWOUD, and S. McDONALD, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM* Comput.Surv.,vol 39,no 1,pp. 1-45,2007.

[17] S.Xu and S.Capkun,Distributed and secure bootstrapping of mobile ad hoc networks:Framework and constructions,"ACM Trans. Inf.Syst.Secure.,vol.12,no. 1.pp. 1-37,2008

[18] S.Zaho and Aggarwal,"Againstmobile attacks in ad hoc networks," in proc.IEEE International Conferences on Information Theory and Information Security,2010.

[19] X. Boyen, "Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography," in *Proc. Crypto 2003*, 2003.

[20] J. Cha and J. Cheon, "An identity-based signature from gap diffie-hellman groups," in *PKC: International Workshop on Practice and Theory in Public Key Cryptography*, vol. 2567. LNCS, 2003

[21] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against olsr: Distributed key management for security," in *Proc. OLSR Interop and Workshop*, 2005.

[22] S. Zhao and A. Aggarwal, "PAPA-UIC: a design approach and a frame-work for secure mobile ad hoc networks," *Security and Communication Networks, John Wiley & Sons*, vol. 1, pp. 371–383, 2010.

[23] B. Lynn, "Authenticated identity-based encryption," Cryptology ePrint Archive, Report 2002/072, Jul. 11 2002.

[24] S. Balfe, K. D. Boklan, Z. Klagsbrun, and K. G. Paterson, "Key refreshing in identity-based cryptography and its applications in manets," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*. IEEE, 2007, pp. 1–8.

[25] K.Hoeper and G. Gong,"Bootstraping security in mobile ad hoc network using identity based scheme with key

revocation," University of Waterloo,report 2006-04,2006.[online].Available:http://www.comsec.uwaterloo.ca/~khoper/IBCrevocation_hoeper.pdf

[26] D. Carman, "New directions in sensor network key management," *International Journal of Distributed Sensor Networks*, vol. 1, pp. 3–15, 2004.

[27] S. Balfe, K. D. Boklan, Z. Klagsbrun, and K. G. Paterson, "Toward hierarchical identity-based cryptography for tactical networks," in *Mili-tary Communications Conference, 2004. MILCOM 2004. IEEE*. IEEE, 2004, pp. 1–8.

[28] F. Li, Y. Hu, and C. Zhang, "An identity-based signcryption scheme for multi-domain ad hoc networks," in *Proc. 5th international conference on Applied Cryptography and Network Security*. Springer-Verlag, 2007, pp. 373–384.

[29] L. Cai, J. Pan, X. Shen, and J. W. Mark, "Peer collaboration in wireless ad hoc networks," in *Proc. 4th International IFIP-TC6 Networking Conference*, ser. LNCS, vol. 3462. Springer, 2005, pp. 840–852.

[30] G. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Proc. ASIACRYPT*. LNCS, Springer-Verlag, 2002.

[31] R. Granger, D. Page, and N. Smart, "High security pairing-based cryptography revisited," in *Algorithmic Number Theory Symposium VII*. Springer-Verlag LNCS 4076, Jul. 2006, pp. 480–494.

[32] E. Verheul, "Evidence that XTR is more secure than supersingular ellip-tic curve cryptosystems," *JCRYPTOL: Journal of Cryptology*, vol. 17, 2004.

[33] D. Moody, "The diffie—hellman problem and generalization of verheul's theorem," *Des. Codes Cryptography*, vol. 52, no. 3, pp. 381–390, 2009

[34] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.