Available online at https://www.asjp.cerist.dz/en/PresentationRevue/134

RIST

Information Processing at the Digital Age Journal

Volume 26, No 1 (2021)

Special issue of

The 2nd International Conference on Computer Science's Complex Systems and their Applications (ICCSA'2021)

A Survey on Identity-based Key Management Schemes in Mobile Ad hoc networks

Kenza Gasmi[a], Abdelhabib Bourouis[a], Rohallah Benaboud[a]

[a] ReLa(CS)[2] Laboratory, Oum El Bouaghi University, 04000, Oum El Bouaghi, Algeria

Abstract

Mobile Ad hoc networks attract more attention over the years, but the security matter of this type of network makes it hard to achieve all of their advantages. Cryptographic key management is the cornerstone for building any robust network security solution. Identity-based cryptography is a promising solution that resists well the key escrow problem, which is suitable for Mobile Ad hoc networks. In this paper, we give an overview of the most important identity-based encryption schemes proposed in the last decade; combined with other techniques to enhance it and provide better results for Mobile Ad hoc networks. Hence, we give a comparative analysis to highlight their advantages and weaknesses. This work gives insights into a recent research to point out its interesting features, take advantages of its strength, ovoid its weaknesses and to lay out the future directions in this area.

Keywords: MANET, key management, identity-based, cryptography, Threshold Cryptography.

1. Introduction

Without any sort of infrastructure, a mobile ad hoc network (MANET) can manage to establish a robust communication, where wireless mobile nodes cooperate as one to keep the network connected. Each one of the network nodes relies on others to reach a destination where all of them act booth as participants as well as routers. Easy and rapid to deploy, self- organizing, low cost and the size of hosts make this type of networks on demand in all domains where a distribution wireless communication needs to be obtained. MANET is widely employed in military, medicine, natural disaster and several other important areas. However, end-to-end communication caused by the absence of infrastructure, bandwidth-limited, the mobility and the short life of nodes decrease the security of the network. The absence of infrastructure and the limited bandwidth enforce the nodes to communicate through others. An intruder can falsify the communication by modifying or deleting the packets, or even inject false ones. Furthermore, attackers can spy the packets in a passive way by analyzing them then extracting information, or use the active way, so they can interrupt the network operations. The mobility makes the topology changes frequently. The nodes enter and exit the network at any time, making hard to establish trust between network members. The short life caused by limited energy incites the selfish behaving, which causes the reject of messages and leads to not reaching the destination. Moreover, a good security algorithm, which probably requires complicated calculations and a lot of energy, will be difficult to adapt.

Many solutions had been proposed to deal with the security requirements of MANETs, but none of them had reached the security level. One of the top security mechanisms is the cryptographic techniques, which can be an ideal choice to establish a general secure framework in Ad hoc networks. The cryptography is a way of making a secret communication between two parties in the presence of an eavesdropping adversary. The cryptography uses mathematical function and a cryptographic algorithm in a combination with a key to decrypt plain text (clear text) to a cipher-text. It uses mathematical technique to encrypt and decrypt information, so no one can discover it if he is not allowed. Unlike what cryptography does, cryptanalysis seeks to break secure communication using the so called attacks by deciphering ciphers without the knowledge of the used keys. There are two basic types of cryptography based on the nature of used keys and are *Symmetric Key* and *Asymmetric Key*. The former is the oldest and easiest type where the same secret key must be shared by all of the communication members. Knowing this key by an attacker threatens the whole communication. For the later, each member of the communicating group uses two different keys or a key pair. One of which everyone knows and called public, and the other must be kept secret and is only known by its owner. For confidentiality purposes, the encryption uses the public key while the decryption uses the private one.

The secrecy of the keys and the strength of the algorithm are the main things that make the data exchange secure. Create, install, update, revoke or even destroy the keys need to be managed. The huge number of keys in a network and the strength of each one of them must be managed using an optimal and a robust mechanism. The key management system is the right mechanism that handles the keying material. Because of the complexity of the key management system, most of the proposed schemes do not target all of its steps. Generally, they focus just on one of the cryptography types, despite the fact that the two are usually required together.

The leading traditional asymmetric scheme that manages the public-key encryption is the public key infrastructure (PKI). It provides secure communication on an insecure public network and uses a digital signature to verify the identity of the entities. The PKI relies on the security of central control point, called the Certification Authority (CA), that everyone trust. In MANETs, one CA is as applying a single point of failure. If this point is compromised, the security of the entire network will fall down. Another obstacle of using PKI in MANETs is the heavy overhead of transmission and storage of Public Key Certificates (PKCs), Zhao et al., 2013.

To avoid the upcoming problems within the PKI, identity based cryptography (IBC) can be a good alternative Shamir, 1984 and Boneh and Franklin, 2001. Here, the asymmetric keys are derived from the user's identity. Thus, there is no need of the CA and the PKCs. Thanks to the reduction in the cost of storage, computation and communication, IBC also adapts to MANETs limited in bandwidth and resources, Zhao et al., 2013.

Instead of CA, another trustworthy authority, called a Private Key Generator (PKG), is needed to generate the private key corresponding to a given identity and can be considered as a single point of failure. Similar to CA in PKI, if the PKG is compromised, the security of the entire network will be exposed. Several revised types of identity-based schemes had been made using multiple authority approaches. Nevertheless, they also caused some other new problems, Zhao et al., 2013.

The threshold cryptography is a complimentary technique to IBC where the secret can be divided into *N* sub-secrets shared by a group of users. Thus, instead of using one PKG node in IBC, *N* nodes can play its role.

The rest of the paper is organized as follows. Section II introduces the concept of key management system. Section III recalls briefly some background knowledge. Section IV reviews the most recent ID-based key management schemes for MANETs in a comprehensive comparative study that highlights strengths and weaknesses. Section V summarizes the weaknesses of the IBC which still pose challenges and require effective solutions. Finally, we conclude this study in Section VI.

2. Key Management System

The establishment of secure communication is crucial in any network. It is a more challenging and hard to achieve task in mobile ad hoc networks than in their wired counterparts. Cryptography is a valuable tool to ensure this goal and implies the use of various small pieces of data known as keys. Keys are themselves sensitive data that need to be securely handled by key management systems (KMS). A KMS is an important process to both traditional and Ad hoc networks when secret communication between any two parties requires handling keys. The use of the keys can be divided in two main types. The first type, that it called symmetric-key, is when all the entities that participate in the communication share the same secret key, where the second uses two different keys per entity. This type is the asymmetric-key. One of its keys is public and used for encryption where the other is secret and used for decryption.

2.1. Key management stages

Key management has to go through several steps to achieve its goals, either in symmetric as well as in asymmetric systems. This process is summarized in Anjum and Mouchtaris, 2007 as follows:

1. Users initialization system: This step bootstraps the system. Non-cryptographic operations are included but others are, such as providing identities to the users, verifying user's information, and ensuring the proper software to the key management process.

2. Creating, distributing and installing the keying material: Keys can be created in a centralized or decentralized manner by the parties that are allowed to that could be the users themselves. Keys must be securely distributed to their owners. All parties involved in a communication based on symmetric cryptography must get securely the same key. In asymmetric cryptography, only the authorized party have to receive the private key in a secure way. The public key has to be delivered to any demanding party preserving integrity and authenticity. After the creation and distribution, the keys can then be installed into the nodes.

3. The use of the keying materiel: In this stage, secure communication can be achieved. Using keys to encrypt data and control the exchanging traffic between the network nodes

4. Updating, revoking, and destroying the keying material: Key management must deal against several threats. Updating keys periodically can avoid attacks that managed to prevail over old ones. Compromised nodes lead to compromised keys that can affect confidentiality, authenticity, and the unauthorized use of keys. In such a case, compromised nodes must be revoked. In some cases, replacement of the keys can be done. Of course, this operation cannot be effective if compromised nodes are under the control of the adversary.

5. Archiving the keying material: This final step may not be always applied. It might be needed only when keys must be saved for auditing purposes, such as in the case of legal proceedings.

2.2. Categories of Key Management Schemes

Key management schemes can be classified in two main categories: contributory and distributive, Marrie et al., 2006. A collaborative effort of two or more nodes results in contributory schemes to agree on a key. In distributive schemes, each node generates a key and tries to distribute it to others. In this paper, we focus on distributive schemes.

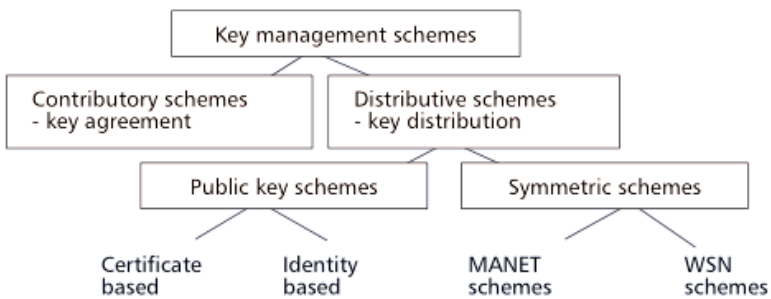

Fig. 1. Classification of key management schemes, Marrie et al., 2006.

As mentioned before and illustrated in figure 1, asymmetric and symmetric cryptography are the main two cryptographic categories for distributed key management schemes. These two types are generally combined with different techniques to solve specific problems or to get more secure. However, key management in ah doc networks is more challenging than in traditional networks. Key management approaches in traditional networks depend on trusted third parties (TTP) that all of the system nodes trust. The use of a TTP can be achieved in three different ways. In-line TTP, which is an active entity that participates not only in deciding the keying material but during the entire communication as well. On-line TTP is an active trusted entity which participates only in deciding the keying material. Off-line TTP is no longer needed to be part of the system after the distribution of the keys. The keys are distributed in the initialization phase when the system is bootstrap.

The TTPs are important pieces in key management schemes to achieve a secure communicating system in traditional networks. However, it is not always applicable to MANETs, due to their main characteristics and to the lack of trusted infrastructure.

1. Symmetric Key-Based Approach: Keys in this approach are loaded into the nodes before the deployment of the system. Secure communication then can be found during the operation of the network using the secret information that are stocked into the nodes. The use of one common key, a shared key between two or more nodes or the use of a random set of keys to each node are basically the approaches on which the existing solution are based. These approaches can be divide in two categories, being either deterministic or probabilistic schemes. In a deterministic scheme, the identity of the nodes and the keys loaded on, have a

deterministic relationship. Moreover, secure link that exists between any two nodes can be predicted exactly. Several options in choosing the keys are used and the basic alternatives are: one common key for the entire network or each node has a separate key for every other node. For the probabilistic technique, a pool of keys is used, and a bunch of keys that are randomly chosen from this pool, are loaded into each node. Thus, a secure link is built with a certain probability between any two nodes provided by common keys shared between them. The probabilistic scheme namely consists of three phases; key pre-distribution where the pool of *P* keys is generated along with the keys identifiers. This pool is generated before the deployment of the nodes by a trusted authority. Then, this authority randomly choses *K* keys among *P* and installs them on each node along with their identifiers. The size of the key pool is chosen in a way that any random collection of *K* keys can at least share one key in common with certain probability. The second phase is the shared key-discovery. Nodes start to discover the shared keys with their neighbors. In the case where common keys exist, nodes can then agree on one of them and establish a secure communication. In the opposite case where no common keys exit, nodes will not be able to establish secure link directly. Note that this phase starts after the installation of the system. The third phase is needed in case of not fully connective system. This phase is called path-key establishment. It is possible that there are no common keys between pair of nodes in the network. In such a situation, nodes without a shared key can get a direct secure link by agreeing on a secrete key using one of the indirect secure paths which are formed by nodes already sharing pairwise keys.

2. Asymmetric Key-Based Approach: The best-known traditional approach of asymmetric cryptography is the public key infrastructure (PKI) where authentic public keys are required to be distributed. A centralized trusted authority or so-called certification authority (CA) guarantees the authenticity of nodes' public keys. In order to do that, this authority makes digital signatures corresponding to the user's public key, using its public/private key pair. Every node in the network is supposed to know its proper public key. Nodes on the network usually send a signed certificate provided by the CA to other parties to confirm their public key when requested. The CA must manage also the expelled nodes, so for any reason certificates can be revoked.

3. Preliminaries

3.1. Identity-based scheme

In Shamir, 1984, the author introduced a new scheme that eliminates the need for certificates. To avoid the trusting problems between the parties in the network, their identities serve as mean to create public keys. With this propriety, Shamir proposed an identity based cryptography (IBC). After Shamir's proposal, several schemes have been presented based on IBC. Unfortunately, none of them was fully satisfactory. Boneh and Franklin, 2001 presented an identity-based encryption scheme (IBE) based on properties of bilinear pairings on elliptic curves, which is the first fully functional, efficient and provably secure identity-based encryption scheme. In the same year, Boneh et al., 2001, proposed a basic signature scheme (BLS) using pairings, that has the shortest length among signature schemes in classical cryptography , Zhao et al, 2007. This type of identity-based cryptography is also named Pairing-based Cryptography (PBC). Based on Boneh and Franklin, 2001; Boneh et al., 2001, a number of schemes has been proposed and most of recent proposals for MANETs in the literature use PBC.

The IBC is a subcategory of asymmetric cryptography. Instead of generating a random public/private pair of keys, each party chooses its keys depending on its identity. For example: name, address or telephone number, making sure that it uniquely identifies the party and it is available at any time for others. The need for a certification authority (CA) and public key certificates (PKCs) are eliminated in IBC. Instead, another trustworthy authority, called a Private Key Generator (PKG), is used to generate the private key corresponding to a given identity as illustrated in figure 2. Before sending private keys, the PKG have to

verify the validity of the user's identity. The keys generated by the PKG are a short-lived in general. Hence, as soon as the private key expires its owner must call a key freshness from the PKG. The sender in addition, must not wary about the expiring time of the receiver private key and it can encrypt any message using the public key at any time. The private key should stop being freshed as soon as the identity of the user is revoked. A copy of all generated private keys is kept by the PKG. For this reason, if it gets compromised all data can be decrypted. Threshold cryptography can be a solution for this problem.

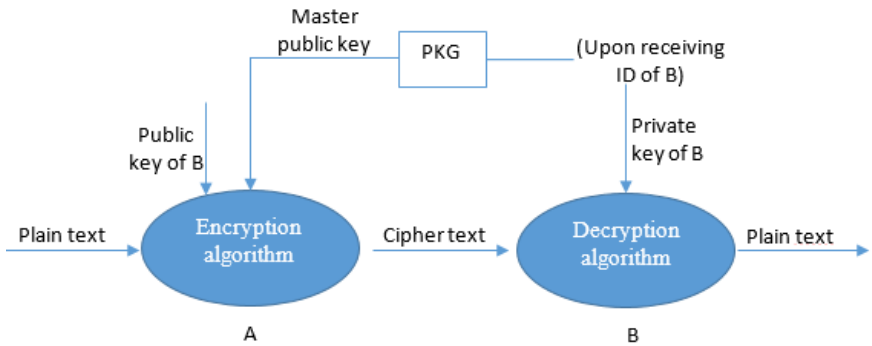

Fig. 2. Identity Based encryption

3.2. Threshold cryptography

Despite the great success achieved by the PKI approach, it is difficult to apply in MANETs for many reasons. A centralized CA is not suitable for this type of networks. This authority can be the single point of failure. If it happens that the CA is compromised, all of the system will fall down. In this case, adversary can sign or revoke any certificate and consequently can impersonate any node. The other case is when the CA cannot be accessible. In such a situation, nodes cannot be able to update or change their keys. Moreover, new nodes will be unable to get their certificates. Replicate the CA can solve the availability problem but can lead to other problems as the compromise of any replica can impact the whole system. Another solution is to distribute the CA service among the network nodes. A group of nodes can share the responsibility of the CA in a distributed where the private key is divided into shares and each node can get one. Approaches that require all the network nodes to play the CA role are not feasible because of the dynamic characteristic of the MANETs. For that reason, threshold cryptography can provide the solution. An *(n, k)* threshold cryptography scheme allows *n* entities to share the ability to perform a cryptographic operation so that any *k* entities suffices to perform this operation jointly, whereas it is infeasible for at most *k-1* entities to do so, even by collusion , Zhou and Haas, 1999. Shamir, 1979 was the first one who came with this idea in 1979. Its proposal was based on polynomial interpolation. To distribute a secret *S* among *n* users, a trust authority chooses a large prime *q*, and randomly selects a polynomial *f* over *q* of degree *k-1*, such that *f (0)=S*. The trust authority computes each user's share using $S_i=f(i) \ mod \ q$ and securely sends the share S_i to user *i*. Then any *k* shareholders can reconstruct the secret using the Lagrange interpolation.

4. ID-Based Key Management in MANETs

In this section, we summarize the most interesting recent proposals in the literature. Table 1 gives an overview of the basic characteristics of the IBC key management schemes. The IBC is often combined with

other techniques for better adaptability.Table 2 shows the capabilities of the keys generation, update and distribution.

The IBC has several advantages. It is presented as a workable solution against the large number of problems related to the public key infrastructure. The private keys are short and they are easy to generate and store. The public keys are implicitly associated with users' identities, with no need to distribute and to store any certificate or the public key of the certification authority. Thus, eliminate the certificate distribution process, the storage and the transmission of the public keys. However, if the private key generator has been compromised, all the packets protected during the lifetime of the public/private key pair used by this server

Table 1. Summary of Identity-Based Key Management Schemes.

Scheme	Focus on/main features	Key Update	Key Agreement	Weaknesses
Xiong and Gong, 2011	• Threshold secret sharing (To resist mobile adversaries attack and ensure availability of network services) • Bilinear Pairing computation (To reduced communication overhead and computational cost) • Elliptic Curve Cryptography ➢ Main goal: construction of three level security communication framework through tree and cluster structure Ad hoc networks.	√	X	• One change needs all system update • Compromising one node threats all lower layer nodes.
Chan, 2011	• Threshold cryptography. • Bilinear pairing Cryptography. ➢ Main goal: eliminating the need of a centralized server.	X	√	• Uses the hardness of discrete logarithm problem which can lead to computational problems and extensive use of many resources.
S.Zhao et al, 2013	• Bilinear pairing Cryptography. ➢ Main goal: eliminating the interdependency cycle between secure routing and security services.	√	X	• One PKG leads to a single point of failure.
Da Silva and Albini, 2013	• Threshold secret sharing (To distribute the PKG task • Bilinear pairing Cryptography ➢ Main goal: creating a complete and fully self-organized ID-based key management scheme for MANETs.	√	X	• Since the number of compromised nodes can reach *t*, the threshold scheme must be *(m,t+1)* instead of (m,t). • Nodes cannot construct functional routes in bigger areas and the system cannot complete all its operations. • The more the threshold *t* increases, the less the system efficiency will be.
Honarbakhsh et al, 2014	• Combination of two unique user's identification parameters *id* and *time*. • Threshold cryptography (To distribute the PKG task). ➢ Main goal: to reduce the possibility of impersonation and enhance the authentication process of user in the network.	√	X	• Need to communicate with PKGs all the time (consume a lot of energy). • The keys are changed all the time.
Pura and buchs, 2014	• A Self-Organized Key Management Scheme. ➢ Main goal: to make the nodes capable of ensuring the credibility of themselves when it is needed in order to communicate in a secure manner.	X	√	• Needs many resources and consumes a lot of energy (share a secret with every other user, which could lead to considerable overhead). • Two successive malicious nodes can easily corrupt the system. • Easy to issue a certificate for a non-existent node, and try to convince the others that such a node does exist in the network.
Yan et al, 2016	• Next generation protected storage of portable trusted platform module (PTPM.next). ➢ Main goal: To resolve the problems of node multiple keys management and protected storage in MANETs.	X	X	• Intensive computations.
Mehr and Niya, 2015	• Key pool. • Pairing based key generation • Threshold cryptography (to distribute the PKG task). ➢ Main goal : eliminating the interdependency cycle between secure routing and security services.	X	√	• All initial nodes are required to generate the master private key. • Lack of authentication, integrity and so on, before the deployment of the IBC system. • Assumption that initial nodes are not malicious.
Mehr and Niya, 2016	• Detailed implementation of Mehr and Niya, 2015.	X	√	• An *(n,n)* threshold cryptography. • All initial nodes are required to generate a new PKG.

Subbulakshmi and Vimal, 2016	• ID + secret value. • Bilinear pairing based cryptography. ➢ Main goal: encryption, decryption and signatures.	√	X	• Too much messages to exchange that consumes a lot of energy. • The refreshment of the keys with Short-Term Refreshment requires to replay the whole process.
Wang and Hu, 2016	• Threshold cryptography. • Multiple variables polynomial. • Intrusion Detect System "IDS" (to select the best nodes to work as the PKG). ➢ Main goal: creating a distributed hierarchical key management scheme where an optimally selected nodes can updates nodes keys easily.	√	√	• Knowing the master secret key of the system exposes the secret keys of all nodes. • Easy to calculate the shared key between two leaf nodes (it is the combination of their identity). • IDS can be a single point of failure.
Chandrashekar and Manoharan,2018	• Threshold cryptography. • Group polynomial equation for generating the unique ID for each node. ➢ Main goal: securely share the secrets, enable a secure and reliable communication, avoid congestion and reduce the overhead.	X	√	• Needs registration with the home network. • The network administrator is a single point of failure.
Rani et al, 2018	• RSA. • AODV-routing protocol. ➢ Main goal: securing data packets and multicasting it in the network.	√	Each group has its own updated common group key	• Not enough details are given • One server which is the single point of failure.

Table 2. Summary of ID-Based Key Generation and Distribution Schemes.

Scheme	Certification Authority	Master Key pair generated by	PKG	Share of private key transmission	Share update
Xiong and Gong, 2011	X	*N* nodes in a distributed manner	Three level PKGs	Private channel.	Cluster nodes.
Chan, 2011	T PKGs	The initial nodes in a distributed manner	*K* among *N*	Private channel	X
S.Zhao et al, 2013	PKG offline	PKG	One PKG	Public channel	PKG
Da Silva et Albini, 2013	Distributed PKG	Nodes that participate in the group initialization called founding nodes	Founding nodes in a distributed manner	Not mentioned	PKG
Honarbakhsh et al, 2014	PKG offline	Not mentioned	*K* among *N*	No transmission, each node creates its own key	The nodes themselves
Pura and Buchs, 2014	X	The nodes themselves	*N*	No transmission, each node creates its own key	X
Yang et al, 2016	PKG Offline	PKG	One PKG	No transmission, each node creates its own key	X
Mehr and Niya, 2015; 2016	PKG Offline	The initial nodes in a distributed manner	Fully distributed	Secret channel	X
Subbulakshmi and Vimal, 2016	X	The nodes themselves	X	No transmission, each node creates its own key	Not mentioned
Wang and Hu, 2016	IDS	The root authority.	Multiple PKGs	X	X
Chandrashekar and Manoharan,2018	X	Not mentioned	X	X	X
Rani et al, 2018	X	Mentioned briefly	X	X	X

are also compromised; which makes the PKG valuable target for adversaries.

To eliminate the single-point of failure, excluding the need of a centralized server in IBC, resist mobile adversaries attack, ensure availability of network services, eliminate the interdependency cycle between secure routing and security services, avoiding congestion and to reduce the overhead, the PKG task is distributed among network nodes throw threshold cryptography. Using *(t,n)* threshold cryptography, only *t* nodes are needed to obtain requesting node keys, thus resisting to the less connectivity problems. The threshold scheme is also used to secure the key generation, distribution and update, which is shown in Table II. In the *(t,n)* threshold scheme the value of *t* must be chosen carefully to ensure security while keeping the service availability, that makes an *(n,n)* threshold system results the maximum security but leads to poor availability.

Furthermore, to ensure a secure transmission of the IBC parameters and reduce the communication overhead and the computational cost, the pairing-based key agreement techniques are used in several proposals. Based on this method and with a few calculation, each two different nodes can agree on a shared secret key that set up a secure link between all network nodes. Another technique used to communicate in a secure manner is a Self-Organized Key Management Scheme. In this scheme, nodes are able of assuring themselves without any sort of authority. The relationships between the nodes are not known beforehand so without depending on the common authority nodes must establish security relationship among themselves after network formation. The proposed scheme in Pura and Buchs,2014 assumes that every node act as a PKG and the trust relationship is bidirectional. Following that manner, the network nodes can only trust their 1-hop neighbors and using this, a trust secure communication is formed.

To support more flexible cryptographic algorithms, encryption systems and node multiple keys, a new identity-based node key management scheme combined with next generation protected storage of Portable Trusted Platform Module (PTPM.next) is proposed in Yang et al., 2016. According to the authors, PTPM is viewed as functionally equivalent to a high-performance USB key. This USB key is used to store, protect and manage a different multiple of keys to support the node multiple keys management schemes. The authors improve PTPM to PTPM.next to support the MANET characteristics.

The hierarchical method has also used in ID-based key management schemes. In this approach, a tree structure is constructed and the depth of the hierarchy is selected. The public/private keys can be deduced

from the root to the leaf or in the opposite direction where the threshold cryptography can be used here. This mechanism is used to improve the network security and to reduce traffic and computation costs.

5. Weaknesses of IBC

Even though the many attractive proprieties of IBC to MANET, there are some problems that steel remains. In this section, we will slightly address some of those problems.

Identity Disclosure: the main idea of the IBC is the identity that can be used as the public key. The problem that can be found is the exposition of the identity to all other nodes. In some networks, this can be a serious issue such as battlefield network.

Key Escrow: the PKG that generates the private key knows all the network private keys and can eavesdrop the traffic or impersonate it. Even this feature can be an advantage in some cases; such as military ; but steel undesirable in others.

Key Revocation: key disclosures are very likely in MANETs due to the weak physical protection of nodes. Frequent rekeying is either computational challenging to solve using distributed on-line key generation or useless with off-line key generation.

6. Conclusion

Over the years, several cryptographic techniques had been proposed in the literature for securing Mobile Ad hoc networks. Identity-based cryptography has emerged recently. It is a special form of PKI which eliminates the need for certificates. In this article, we discussed the important identity-based key management schemes for MANATs proposed in the last decade. Most of the proposals manage to enhance this technique by combining it with various mechanisms, so they can improve it and benefit from their advantages to make it more suitable for MANETs. The comparative study we conducted has revealed many advantages together with some drawbacks and challenges that still need to address.

In the area of securing MANETs, the IBC is widely applied and is a promising solution. However, there are no perfect solutions yet because of the unaddressed issues. Therefore, an important step that cryptography and security engineers should focus on, is to explore deeper in these research areas and try to establish a general key management framework.

As a future work, we attempt to survey the large applications of IBC, not only in key management but also in other areas. Also, we will try to take benefits of this work to come up with a new idea choosing the best techniques to give a better solution for securing the MANETs.

References

K. Zhao, L. Huang, H. Li, F. Wu, J. Chu, and L. Hu, “A survey on key management of identity-based schemes in mobile ad hoc networks,” Journal of Communications, vol. 8, no. 11, pp. 768–779, 2013.

A. Shamir, “Identity-based cryptosystems and signature schemes,” in Workshop on the theory and application of cryptographic techniques. Springer, 1984, pp. 47–53.

D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Annual international cryptology conference. Springer, 2001, pp. 213–229.

F. Anjum and P. Mouchtaris, Security for wireless ad hoc networks. John Wiley & Sons, 2007.

H. Anne Marrie, W. Eli, M. Stig F, R. Chunming, K. Oivind, and S. Pal, “A survey of key management in ad-hoc networks,” IEEE Communications surveys & tutorials, vol. 8, no. 3, pp. 48–66, 2006.

D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” in International conference on the theory and application of cryptology and information security. Springer, 2001, pp. 514–532.

S. Zhao, A. Aggarwal, R. Frost, and X. Bai, “A survey of applications of identity-based cryptography in mobile ad-hoc networks,” IEEE Communications surveys & tutorials, vol. 14, no. 2, pp. 380–400, 2011.

L. Zhou and Z. J. Haas, “Securing ad hoc networks,” IEEE network, vol. 13, no. 6, pp. 24–30, 1999.

A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

W. A. Xiong and Y. H. Gong, “Secure and highly efficient three level key management scheme for manet,” WSEAS Transactions on Computers, vol. 10, no. 1, pp. 6–15, 2011.

A. C. Chan, “Distributed private key generation for identity based cryptosystems in ad hoc networks,” IEEE Wireless Communications Letters, vol. 1, no. 1, pp. 46–48, 2011.

S. Zhao, R. Kent, and A. Aggarwal, “A key management and secure routing integrated framework for mobile ad-hoc networks,” Ad Hoc Networks, vol. 11, no. 3, pp. 1046–1061, 2013.

E. da Silva and L. C. P. Albini, “Towards a fully self-organized identity-based key management system for manets,” in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2013, pp. 717–723.

S. Honarbakhsh, L. B. A. Latif, B. Emami et al., “Enhancing security for mobile ad hoc networks by using identity based cryptography,” International Journal of Computer and Communication Engineering, vol. 3, no. 1, p. 41, 2014.

M. L. Pura and D. Buchs, “A self-organized key management scheme for ad hoc networks based on identity-based cryptography,” in 2014 10th International Conference on Communications (COMM). IEEE, 2014, pp. 1–4.

G. Yang, J. Liu, and L. Han, “An id-based node key management scheme based on ptpm in manets,” Security and Communication Networks, vol. 9, no. 15, pp. 2816–2826, 2016.

K. A. Mehr and J. M. Niya, “Securing mobile ad hoc networks using enhanced identity-based cryptography,” ETRI Journal, vol. 37, no. 3, pp. 512–522, 2015.

K. Adli Mehr and J. Musevi Niya, “Security bootstrapping of mobile ad hoc networks using identity-based cryptography,” Security and Communication Networks, vol. 9, no. 11, pp. 1374–1383, 2016.

P. Subbulakshmi and S. Vimal, “Secure data packet transmission in manet using enhanced identity-based cryptography (eibc),” International Journal of New Technologies in Science and Engineering, vol. 3, no. 12, pp. 35–42, 2016.

F. Wang and S. Hu, “A novel key management scheme for secure mobile ad hoc networks,” 2016.

J. Chandrashekar and A. Manoharan, “An identity based key management technique for secure routing in manet,” International Journal of Intelligent Engineering and Systems, vol. 11, no. 6, pp. 33–43, 2018.

M. S. Rani, R. Rekha, and K. V. N. Sunitha, “Id based multicast secret-key management scheme (skms) in manets,” International Journal of Intelligent Engineering and Systems, vol. 11, no. 6, pp. 199–208, 2018.