ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 3 (July - Sept. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Manet Distributed Access Control and Location Management Using The Scheme of Identity Based Cryptography

[I]Dr. E. Karthikeyan, [II]B. Iswarya
[I]Associate Professor, Dept. of Computer Science, Government Arts College, Udumelpet.
[II]Research Scholar, Government Arts College, Udumelpet.

Abstract
Since the nodes in a MANET have limited resources, designing methods for cryptographic key management is particularly challenging. Because the network infrastructure is unstable, assuming that authorities used in key management are implemented using any single node is not realistic. Threshold cryptography can be used to distribute an authority, such that it is implemented by multiple nodes. This makes the authority more robust against network failures and harder to compromise.
Due to the distributed and dynamic nature of MANETs, it is possible to show that there is a security benefit to be attained when the node states are considered in the process of constructing a private key generator (PKG). In this paper, we propose a distributed hierarchical key management scheme in which nodes can get their keys updated either from their parent nodes or a threshold of sibling nodes. The dynamic node selection process is formulated as a stochastic problem and the proposed scheme can select the best nodes to be used as PKGs from all available ones considering their security conditions and energy states.
Threshold cryptography and identity-based cryptography are found to result in very efficient key management systems, compared to other methods. It is however important to consider which security properties a distributed authority has, especially with respect to any leakage of information on the authority's secret key. However, the main challenge in connection with key management in a MANET is to authenticate nodes without requiring pre-established trust. The proposed scheme can decrease network compromising probability and increase network lifetime in tactical MANETs.

Keywords
MANET, Cryptography, Key Management, Public Key, Threshold.

I. Introduction

A MANET is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Due to the limited transmission range of each mobile node, it may be necessary for one mobile node to enlist the aid of other nodes in forwarding a package to its destination. Therefore, in such environment, every node in the network plays the role of a router by being able to determine the paths of transmitting packets to their destinations. Figure 1.1 illustrates an example of a MANET which contains two laptops, two PDAs and two digital cameras. Since node D is outside node A's transmission range, the data from A to D must be retransmitted by nodes B and C.
MANETs inherit common characteristics found in wireless networks in general, and add characteristics specific to ad hoc networking.

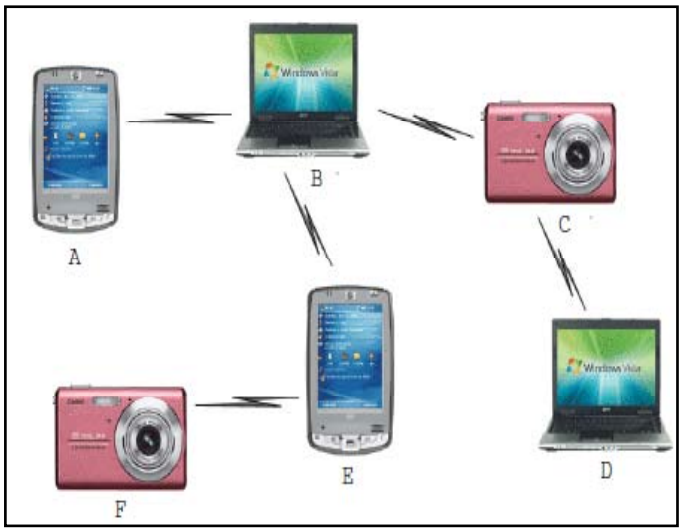

Fig 1.1: A Mobile Ad Hoc Network

The MANETs generally have the following characteristics:

- Autonomous and infrastructureless: A MANET does not depend on any established infrastructure or centralized administration. Each node operates in a distributed peer-to-peer mode, acts as an independent router, and generates independent data.
- Dynamic Network Topology: Each node is free to move about while communicating with other nodes. The topology of such an ad hoc network is dynamic in nature due to constant movement of the participating nodes, causing the intercommunication patterns among nodes to change continuously.
- Wireless Connections and Multi-hop Routing: Nodes communicate through wireless connections and share the same media (radio, infrared, etc.). In order to be able to communicate with devices that are out of range, intermediate devices will forward data packets in a hop-by-hop fashion.
- Resource and Energy Constrained Devices. Most mobile devices are equipped with cheap and slow processors and limited storage capability. In addition, mobile devices generally rely on batteries as their power source. The use of complex algorithms there may not be possible.
- Limited Physical Security. The use of wireless communication and the exposure of the network nodes increase the possibility of attacks against the network. Due to the mobility of the nodes, the risk that nodes are physically compromised by theft, loss, or other means will probably be bigger than for traditional network nodes.

The dynamic and self-organizing nature of MANETs makes them particular useful in situations where rapid network deployments are required or it is prohibitively costly to deploy and manage network infrastructure.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A. Classification of Routing Protocols

The Routing Protocols for ad hoc wireless networks can be divided into three categories based on the routing information update mechanism. They could be Reactive (On-demand), Proactive (Table-driven) or Hybrid.

Figure 1.2 shows the three categories of Ad hoc RPs and various proposed Protocols under each category. The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired.

This is not the case, however, for on-demand routing protocols. When a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed.

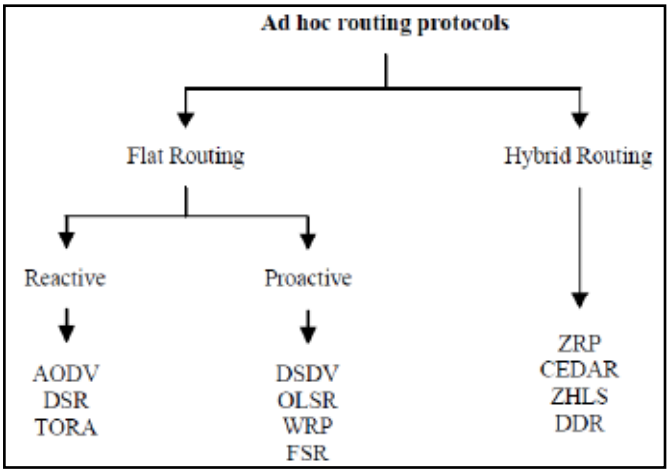

Fig. 1.2: Classification of Routing Protocols

These protocols always maintain up-to-date information of routes from each node to every other node in the network.

The reactive or on-demand routing protocols are based on Query-Reply topology in which they do not attempt to continuously maintain the up-to-date topology of the network.

II. Security in Manets

A MANET provides network connectivity between mobile nodes over potentially multihop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network-layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination. The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination.

Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories: *routing attacks* and *packet forwarding attacks*, based on the target operation of the attacks. The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviors are related to the routing protocol used by the MANET.

There are two mainly protocols are used in MANET networks, Link layer protocol are used to provide connectivity between different mobile nodes in order to ensure one-hop connectivity by using multihop wireless channels. On the other hand if we like to extend connectivity to different multiple hops then MANET network uses network layer protocols. In the coordination process distributed protocols typically assume that all mobile nodes are cooperating with respect to communication but actually this assumption is not possible in hostile mobile networks environment because cooperation is not enforced in MANET.

The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multifence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats. This new design perspective is what we call *resiliency-oriented* security design.

III. Cryptography in Manets

Cryptography is very strongly tied to mathematics and number theory. It is, therefore, difficult to create a new design using composite cryptographic techniques without the sound security analysis behind it, usually based on cryptographic reasoning. One way to reach this goal is to learn from others by reviewing the current MANET security schemes, and also to understand the network to further understand how cryptographic techniques combine with MANETs to provide a security service with reasonable network performance, scalability, storage, and synchronization. Certainly the security design can be evaluated using different techniques. Our goal is to provide perspective using cryptographic techniques and study basic cryptographic techniques when applied to authentication, trust, and key management in MANETs/WSNs. Furthermore, we can study several of the most commonly-used cryptographic techniques and see how they are employed to deal with different tasks and balance security and performance.

Key management is a basic part of any secure communication. Most cryptosystems rely on some underlying secure, robust, and efficient key management system. Secure network communications normally involve a key distribution procedure between communication parties, in which the key may be transmitted through insecure channels. A framework of trust relationships needs to be built for authentication of key ownership in the key distribution procedure. While some frameworks are based on a centralized trusted third party (TTP), others could be fully distributed. For example, a certification authority (CA) is the TTP in asymmetric cryptosystems, a key distribution center (KDC) is the TTP in the symmetric system, and in PGPno TTP is assumed. According to recent publications, the centralized

approach is regarded as inappropriate for MANETs because of the dynamic environment and the transient relationships among mobile nodes. Most researchers prefer the decentralized trust model for MANETs. Several decentralized solutions have been proposed in recent papers with different implementations, such as how the CA's responsibility is distributed to all nodes, or to a subset of nodes.

Cryptographic algorithms are security primitives that are widely used for the purposes of authentication, confidentiality, integrity, and non-repudiation. Most cryptographic systems require an underlying secure, robust, and efficient key management system. Key management is a central part of any secure communication and is the weakest point of system security and the protocol design. A key is a piece of input information for cryptographic algorithms. If the key was released, the encrypted information would be disclosed. The secrecy of the symmetric key and private key must always be assured locally. The Key Encryption Key (KEK) approach could be used at local hosts to protect the secrecy of keys. To break the cycle (use key to encrypt the data, and use key to encrypt key) some non-cryptographic approaches need to be used, e.g. smart card, or biometric identity, such as fingerprint, etc. Key distribution and key agreement over an insecure channel are at high risk and suffer from potential attacks. In the traditional digital envelop approach, a session key is generated at one side and is encrypted by the public-key algorithm. Then it is delivered and recovered at the other end.

The key management schemes in MANET can be classified into three types. It can be described below:

• Asymmetric key Management Scheme

Most of them are based on public-key cryptography. The basic idea is to distribute the CA's functionality to multiple nodes.

• Symmetric key Management Scheme

The basic idea is that each node is preloaded with a set of keys from a large key pool. The key pattern should satisfy the property that any subset of nodes can find at least one common key, and the common key should not be covered by a collusion of a certain number of other nodes outside the subset.

• Group key Management Scheme

Collaborative and group-oriented applications in MANETs are going to be active research areas. Group key management is one of the basic building blocks in securing group communications. However, key management for large dynamic groups is a difficult problem because of scalability and security.

IV. Identity Based Cryptography

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

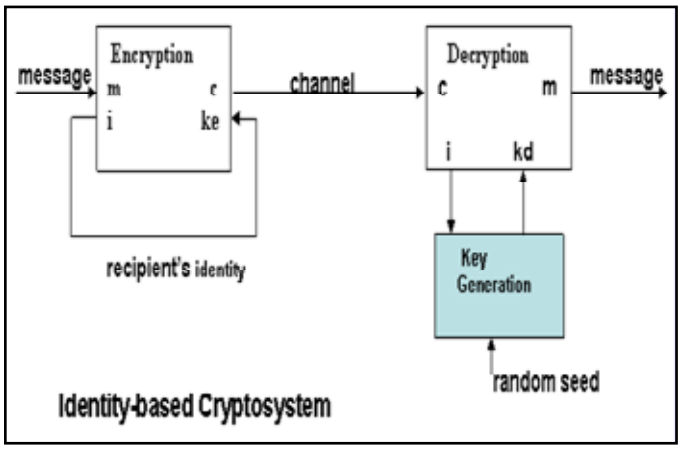

Fig. 4.1: Example of Identity Based Cryptography

The vast majority of proposed identity-based cryptography schemes and certainly all of those discovered so far that are computationally efficient, are based on mathematical functions called *bilinear non-degenerate maps*. A bilinear non-degenerate map is a function pairing elements from one cyclic group to another of the same prime order, where the discrete log problem is hard in the first group.

The security of identity-based cryptography is based on the assumption that the particular bilinear maps chosen are one-way functions, meaning it is easy to calculate their result given a pair of operands but hard to calculate the inverse. This property is often referred to as the *Bilinear Diffie-Hellman Assumption*, since the Bilinear Diffie-Hellman problem is reducible (algorithmically equivalent) to the discrete-log or inverse operation for these bilinear maps.

In simplified notation, a bilinear map is a pairing that has the property:

Pair ($a \cdot X, b \cdot Y$) = Pair($b \cdot X, a \cdot Y$)

In two of the more well-known IDE systems, the Weil (pronounced *vay*, rhyming with the English word *way*) and Tate pairings, the $\cdot$ operator above refers to multiplication of a point on an elliptic curve by integers. Although the multiplication operation, such as calculating $a \cdot X$, is easy, finding a given X and $a \cdot X$ is computationally infeasible.

Boneh and Franklin were the first to propose a viable IDE system based on the Weil pairing in 2001, nearly two decades after Shamir's original proposal. Since that time a number of other pair based IDE and IDS systems have been proposed. Since most of these are pairing-based, identity based cryptography is often called *pairing-based cryptography*.

Cryptographic operations in the Boneh and Franklin IDE system are conducted as follows. Note that some details of the math involved in elliptic curves have been omitted for clarity's sake:

- ***Setup*:** The PKG picks an elliptic curve, a secret s and a point P on the curve using a random number generator. It then publishes P and $s \cdot P$ as the master public key.
- ***Encryption*:** Alice hashes the chosen identity attribute for Bob to a point *IDBob* on the elliptic curve. She then picks a random r and calculates a key k:
  k = Pair($r \cdot IDBob, s \cdot P$)
  Alice then sends Ek[M] and $r \cdot P$ to Bob.
- ***Decryption*:** Bob may not yet have a private key. To get it, he authenticates with the PKG, which calculates $s \cdot IDBob$ and returns it to him over a secure channel. This is his private key. After receiving Ek[M] and $r \cdot P$ fromAlice, Bob can

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

recover the key k by calculating:

$k = \text{Pair}(s \cdot IDBob, r \cdot P)$

This is possible because of the properties of bilinear maps. Bob can then use k to decrypt the message. No one else (besides the PKG) can calculate k because only Bob knows $s \cdot IDBob$. Even though Shamir had already provided one possible identity-based signature system based on RSA in his seminal proposal, other researchers have since discovered pairing-based IBS systems to complement the pairing-based encryption systems. One of the first such systems was proposed by Boneh, Lynn and Shacham.

Most of the identity-based cryptographic schemes which have been proposed up to now employ bilinear pairings, which are maps e: G X G → GT, for groups G (additive) and GT (multiplicative) of the same prime order q, with the following properties:

1. Bilinear: e (aP, bQ) = $e(P,Q)^{ab}$, for all P,Q € G, a, b € Zq.
2. Non-degenerate: $e(P, P) \neq 1_{GT}$ for all P € G.
3. Computable: there exists an efficient algorithm to compute e(P,Q) for any P,Q € G.

A. Setup

An additive group G of prime order q (generated by some public element P) and a multiplicative group GT of the same order are chosen admitting a bilinear pairing e: G X G → GT. Three hash functions H_1: {0, 1}* → G, H_2: GT → {0, 1}^{l} and H_3: G X {0, 1}^{l} → G are needed, where l is the bit-length of the messages to be encrypted.

The master entity has a secret key s € Zq which is chosen at random; the matching master public key is the element PK = sP € G.

B. Key Generation

Assume that the group SG has n users, SG = {P1, . . .,Pn}. Let t^l be the decryption threshold such that $1 \leq t^l \leq n$. If IDSG is the public identifier of the group, then the master entity first computes the matching secret key SK_{SG} of the group as SK_{SG} = sH1 (IDSG) € G. Then, he picks $R_1, \ldots, R_t$10-1 at random from G, and defines the mapping

$$R(z) = \mathrm{SK}_{SG} + zR_1 + \cdots + z^{t^l-1}R_{t^l-1} \in \mathbb{G},$$

Where the variable z takes values in Zq. Each user Pi € SG is (publicly) assigned to a different value zi € Zq.

C. Encryption

Given a message m € {0, 1}^{l} to be encrypted and addressed to the group SG, the sender chooses uniformly and at random r € Zq. Then he computes the value K = e(PK, $H^1(ID_{SG})^r$ and the triple of values U = rP, V = H_2(k) ¤ m, W = rH_3(U,V) which define the resulting ciphertext C = (U,V,W).

D. Threshold Cryptography

Practical cryptographic systems rely on the secrecy of keys to achieve any security. These keys may well be protected by encryption under other keys, but these encryption keys must also be protected. In the end, we must rely on that some keys are stored in a physically secure way.

More risk is associated with the storage of some keys than others. In a PKI, the whole system is compromised if the private key of the CA is compromised. This also holds true for the master-key of the PKG in an IBC system. In a MANET, it is not always plausible to assume that any one node is physically secure. If a node holds the secret key corresponding to the public parameters of the system, an adversary may compromise the whole system by capturing one node. We are therefore particularly concerned that privileged keys are kept secret.

But privileged keys also need to be available. In an IBC system, the secret key corresponding to the system parameters is needed in order to generate keys for nodes. In a PKI, it is needed to generate certificates and revocation lists.

At first, the secrecy and availability requirements may seem contradictive: if we spread the key out on many locations to make it easily available, secrecy is degraded since the key is more prone to get compromised by an adversary. Threshold cryptography solves this problem by offering both secrecy and availability of information at the same time. Two important models for threshold cryptography are secret sharing and function sharing.

1. Secret Sharing

A threshold secret sharing scheme consists of a probabilistic algorithm, called the dealer, that takes as input a secret s, and outputs n shares s1, s2. . . sn. A threshold t, with $t \in [1, n-1]$, is also defined. The idea is that any t shares reveal no information about the secret s, while any t + 1 share determines uniquely.

2. Function Sharing

Secret sharing is a very powerful and versatile tool. However, if it is to be used to share a private key in a practical scenario, a problem arises: the combiner obtains the whole secret key when it is used in some computation. So if the adversary can capture the combiner, he may also compromise the private key. Thus, secret sharing is very useful for secure physical storage of a secret, but as soon as the secret is to be used, it is again very vulnerable to a compromise.

Some thought on this issue reveals that we do not really need to know the private key explicitly as long as we may use it in a calculation of some function. For example, the function could be to sign a public key certificate or generate a private key for a user as a PKG.

V. Results & Discussions

In this section, we illustrate some of the performance benefits of our proposed scheme. An initial simulation scenario has one parent node and five heterogeneous child nodes, each with different transition probabilities, states, and cost matrices. We increase the number of nodes up to 30 in different simulation scenarios. We compare the performance of the proposed scheme with an existing scheme, in which PKG nodes are selected randomly without consideration of the security context.

A brief security analysis of the proposed scheme is given as follows. Our scheme has at least the same level of security as that in the existing node selection schemes for ID-based (k, n)-threshold key management in MANETs, since all of them use the same ID-based public/private keys and threshold cryptography. However, most of existing schemes do not consider how to dynamically select k nodes among the n nodes with master key shares at each time instant taking into account the nodes' security conditions and energy states. Due to the distributed nature of MANETs, a node's security state can change dynamically; some nodes may be in a safe state while others may be under attack by adversaries. Since adversaries can do cryptanalysis on the nodes with master key shares, these nodes would be compromised, and the security of the whole network is breached when a threshold number of shareholders are compromised.

i) Cost Analysis

We perform simulations with 400 steps for 20 times and calculate the average cost of each time slot. Fig. 6.3 shows the cost comparison over the existing scheme when the first component in the state transition probability matrix changes from 0.85 to 0.98. With the increase of the transition probabilities (which is the probability that the node remains in its current state), the system becomes more secure and the proposed scheme always has lower cost than the existing scheme.

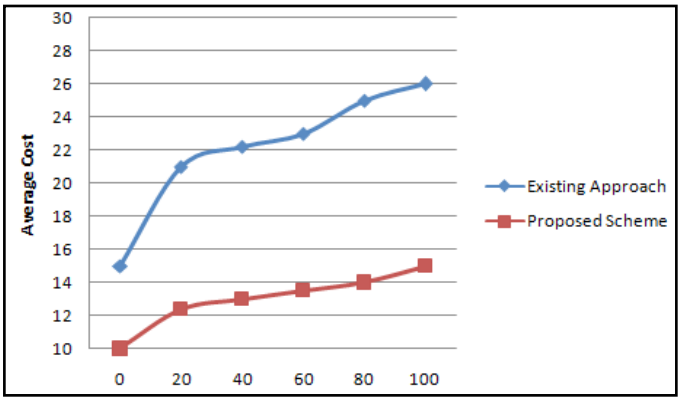

Fig. 5.1: Cost Comparison of availability of nodes

ii) Comparison Key Extract

However, our test shows its performance is quite low. Even if the master key length is only 256 bits, the encryption/decryption speed is below 1KB/s, which cannot be acceptable in most cases. Moreover, the size of ciphertext is thousands times that of plain text.

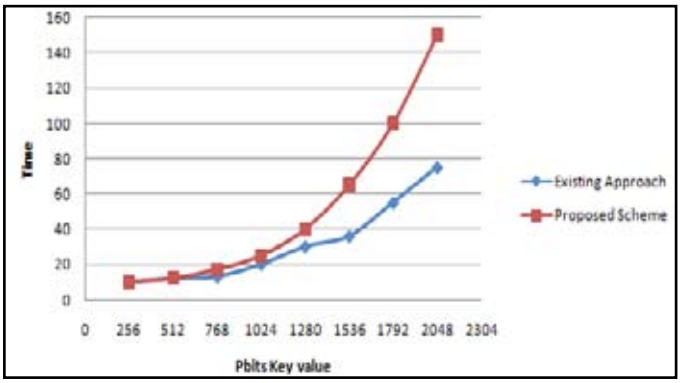

Fig. 5.2 : Key extraction from nodes

iii) Encryption Time

IBC require nodes to obtain authentic system parameters. But as soon as a node has obtained these, it may encrypt to all other nodes, and also check signatures generated by all other nodes — no certificates are required. The only requirement is that the node knows the identity of the other nodes.

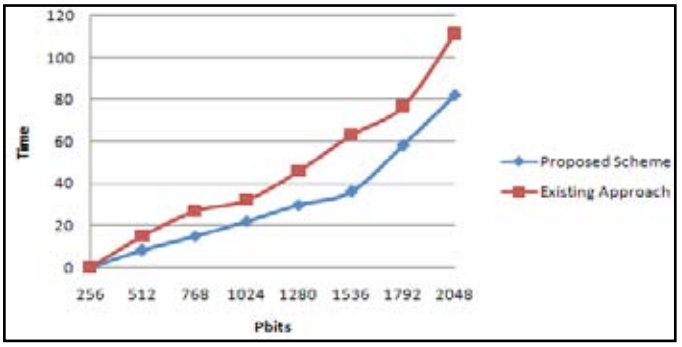

Fig. 5.3 : Encryption Time from nodes

iv) Decryption Time

In an IBC, the PKG will know the private keys of all the users, so the PKG is more trusted in this sense. Furthermore, when the private key of a user is to be issued from the PKG, a confidential channel must be available. Otherwise, the private key may be compromised. This is not a problem in a PKI because only public keys are transmitted.

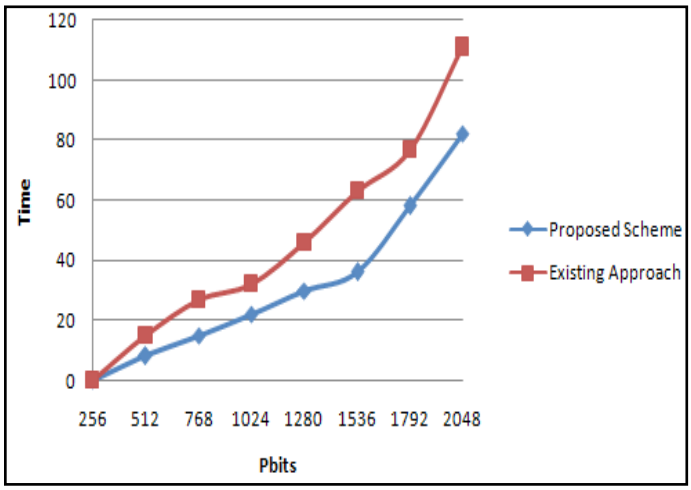

Fig. 5.4 : Decryption Time from nodes

We summarize our discussion with the main advantages and disadvantages of the sketched method for authenticating founder nodes.

VI. Conclusions

All security mechanisms applied in networking more or less require the use of cryptography, which on the other hand implicates a strong demand for secure and efficient key management mechanism. In ad hoc networks the role of a dependable key management service is especially emphasized, given the constrained resources and possibly rapidly varying conditions in which the nodes operate. Traditional and centralized approaches cannot often be applied in the environments in which ad hoc networks operate, which force the use of distributed services that do not rely on single resources with respect to other nodes or communication paths.

In identity based cryptography, it is the Private Key Generator (PKG) that issues keys corresponding to identities. In order to support the self-configuring property of a MANET, the PKG must be online to issue keys to joining nodes. To protect the master-key of the PKG, but at the same time keep it available, we studied the theory of threshold cryptography, including secret sharing and function sharing. The PKG is involved in the Setup and Extract algorithms of an IBC system, so we focused on the distribution of these. But in addition, we discussed how signatures may be generated using a secret sharing of the master-key. This may be used to sign a message as the PKG authority, which is useful for instance when creating revocation lists. But we did not find any definition of security for distributed versions of Setup and Extract.

References

[1] *C. Adjih, T. Clausen, A. Laouiti, P. M¨uhlethaler, and D. Raffo. Securing the OLSR protocol. In IFIP Annual Mediterranean Ad Hoc Networking Workshop, pages 25–27, 2003.*

[2] *M. Akane, H. Kato, Y. Morikawa, Y. Nogami, and Y. Sakemi. Integer Variable _-Based Ate Pairing. In Pairing 2008,*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

volume 5209 of Lecture Notes in Computer Science, pages 178–191. Springer-Verlag, 2008.

[3] T. R. Andel and A. Yasinsac. Surveying Security Analysis Techniques in MANET Routing Protocols. IEEE Communications Surveys & Tutorials, 9(4):70–84, 2007.

[4] P. G. Argyroudis and D. O'Mahony. Secure Routing for Mobile Ad hoc Networks. IEEE Communications Surveys & Tutorials, 7(3):2–21, 2005.

[5] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for Key Management — Part 1: General (Revisited). NIST Special Publication 800-57, March 2007.

[6] D. Beaver. Foundations of Secure Interactive Computing. In Advances in Cryptology – CRYPTO '91, volume 576 of Lecture Notes in Computer Science, pages 377–391. Springer-Verlag, 1992.

[7] M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In ACM Conference on Computer and Communications Security, pages 62–73, 1993.

[8] I. F. Blake, G. Seroussi, and N. P. Smart, editors. Advances in Elliptic Curve Cryptography, volume 317 of London Mathematical Society Lecture Note Series. Cambridge University Press, 2005.

[9] G. R. Blakley. Safeguarding cryptographic keys. In Proc. AFIPS 1979 National Computer Conference, volume 48 of AFIPS Conference proceedings, pages 313–317. AFIPS Press, 1979.

[10] A. Boldyreva. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In International Workshop on Practice and Theory in Public Key Cryptography, volume 2567 of Lecture Notes in Computer Science, pages 31–46. Springer-Verlag, 2003.

[11] D. Boneh and M. Franklin. Efficient generation of shared RSA keys. Journal of the ACM, 48(4):702–722, July 2001. 96 REFERENCES

[12] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In Advances in Cryptology – CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, 2001.

[13] D. Boneh, C. Gentry, and M. Hamburg. Space-Efficient Identity Based Encryption Without Pairings. In 48th Annual IEEE Symposium on Foundations of Computer Science, pages 647–657. IEEE Computer Society, 2007.