Survey of key management in Mesh based Multicast MANET

[1]Purvi Ramanuj, [2]Dr. J S Shah
[1]Ph. D. Scholar, School of Engineering, R. K. University, Rajkot, India
[2]Principal, Gujarat Institute of Technical Studies, himmatnagar, Gujarat, India

Abstract - Mobile ad hoc networks (MANETs) are more vulnerable to security attacks compared to the wired networks mainly because they are wireless and dynamic in topology. So security has become a primary requirement for successful operation. Achievement of key goals like confidentiality, access control, authentication, availability, integrity, and non-repudiation is very crucial. Cryptographic techniques using cryptographic keys are widely used for secure communications. It becomes very crucial to provide secured and efficient key management scheme as well as all the messages should also be secured. A number of key management schemes are proposed in MANET. The computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. We hereby present a comprehensive study of various key management techniques available for MANET.

***Keywords* - Mobile Adhoc network; ID Based Security; Mesh based Multicast; Key management**

I. INTRODUCTION: MOBILE AD HOC NETWORK

Mobile ad-hoc network (MANET) is an infrastructure less collection of mobile devices which are connected by wireless links. MANET nodes move from one place to another and change their configuration dynamically. Connectivity among nodes changes as some nodes may leave the network while some may join the network. This results into dynamic topology changes. Each node is a host as well as a router. Thus there is no fixed communication structure and also no base station which organizes communication pattern.

A. Multicast Routing Protocols

Routing plays an important role in operation of MANTEs. Depending on the nodes involved in the communication, there are three types of routing: Unicast – a sender sends data to a single node, Broad cast – a sender sends data to all in the network and Multicast – a sender sends data to a group of users. Multicast routing protocols play an important role in MANET to provide video Conferencing, civilian operations, e-education, classroom meetings and emergency search-and-rescue. In MANETs environment, for efficient use of bandwidth, multicast is used rather employing multiple unicast. Depending on the underlying topology the multicast protocols are mainly classified as tree-based and mesh-based protocols. In tree-based protocols only one route exists between a source and destination and hence these protocols are efficient in terms of the number of link transmissions. There are two major categories of tree-based protocols: source tree-based e.g. BEMRP, DDM, MCEDAR, ADMR and shared tree-based e.g. MAODV, AMRIS. Shared tree-based multicast protocols are more scalable with respect to the number of sources, but suffer under a single point of failure, the core node. In mesh-based multicast routing, multiple routes exist between the source node and each of the receivers of the multicast group. A receiver node receives several copies of the data packets, one copy through each of the multiple paths. Mesh -based multicast routing protocols provide robustness in the presence of node mobility, however at the expense of a large number of link transmission leading to inefficient bandwidth usage. The mesh-based protocols are classified into source initiated e.g. ODMRP, DCMP, NSMP, ACMRP and receiver initiated e.g. MANSI protocols depending on the entity that initiates mesh formation[1].

B. Security

Because of their wireless and dynamic nature, security is one of the most important issues in communication in MANETs. Security services include the functionality that is required to provide a secure networking environment. It comprises authentication, access control, confidentiality, integrity, non repudiation, and availability[10]. Authentication is the ability to verify that a peer entity in an association is the one it claims to be, or can be used for the determination of data origins. Availability ensures the survivability of the network service despite denial of service attacks. Confidentiality ensures that certain information is never disclosed to unauthorized entities. Integrity guarantees that a message being transferred is not corrupted. Non-repudiation ensures that the origin of a message cannot deny having sent the message. Access control is the ability to limit and control access to devices and/or applications via communication links.

Cryptography is an important and powerful tool for secure communications. It transforms readable data (plain text) into meaningless data (cipher text). Cryptography has two dominant categories, namely symmetric-key (secret-key) and asymmetric-key (public-key) approaches [16]. In symmetric-key cryptography, the same key is used to encrypt and decrypt the messages, while in the asymmetric-key approach, different keys are used to convert and recover the information. The asymmetric cryptography approaches are versatile and can provide services like authentication, integrity, and privacy. They are also simpler for key distribution compared to the symmetric approaches. Symmetric-key algorithms are generally more computation-efficient than the asymmetric cryptographic algorithms. There are varieties of symmetric and asymmetric algorithms available, including DES, AES, IDEA, RSA, and EIGamal. Threshold cryptography is another cryptographic technique that is quite different from the above two approaches. In Shamir's (k, n) secret sharing scheme, secret information is split into n pieces according to a random polynomial. The secret could be recovered by combining any threshold k pieces based on Lagrange interpolation.

II. KEY MANAGEMENT

Any Multicast routing protocol requires to secure the multicast sessions from intruders or from any other illegal operations. Key management plays an important and vital part of any secure communication. Most of the crypto systems rely on underlying secure, robust, and efficient key management system in one or the other way. Generated keys are distributed to communicating nodes mostly through insecure channels. A centralized trusted third party (TTP), or a fully distributed system or a right combination of both is used for authentication of key ownership in the key distribution procedure. For example, a certification authority (CA) is the TTP in asymmetric cryptosystem, a key distribution center (KDC) is the TTP in the symmetric system, and in PGP no TTP is assumed. Also a threshold cryptography has become verey popular in recent past. The basic idea is to distribute the CA's functionality to multiple nodes. It employs (t, n) threshold cryptography. The system can tolerate t-1 compromised servers. In localized key management scheme all nodes are servers and the certificate service can be performed locally by a threshold number of neighboring nodes. A fully distributed scheme provided a composite trust model.

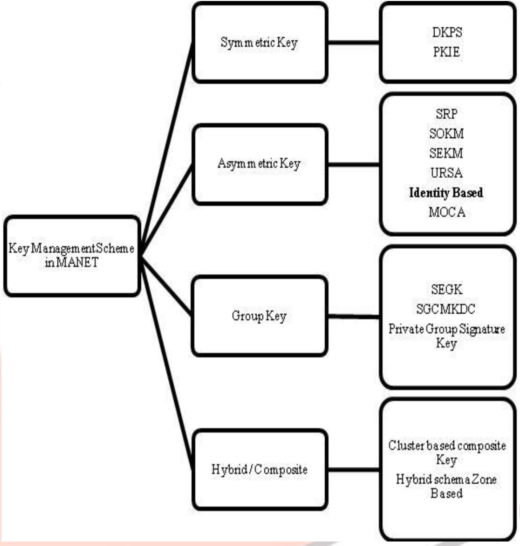

Figure 1 Key Management Schemes in MANETs

A. *Symmetric Key Management*

Symmetric key management schemes were initially proposed for sensor nodes that are assumed to be incapable of performing costly asymmetric cryptographic computations. Pair wise keys can be preloaded into nodes, or based on the random key distribution in which a set of keys is preloaded. 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.

Distributed Key Pre distribution Scheme (DKPS) - DKPS [6]is aimed at the network settings where mobile nodes are not assumed to be capable of performing computationally intensive public key algorithms and the TTP is not available. The basic idea of the DKPS scheme is that each node randomly selects a set of keys in a way that satisfies the probability property of cover -free family (CFF). Any pair of nodes can invoke the secure shared key discovery procedure (SSD). The theory behind the SSD is the additive and scalar multiplicative homomorphism of the encryption algorithm as well as the property of non-trivial zero encryption. To discover the common secret key, one side of the two parties can form a polynomial and send the encrypted polynomial to the other side. The coefficients of the polynomial are encrypted with the sender's secret key. The other side will send back the encrypted polynomial multiplied by a random value. Because of the homomorphism and non-trivial zero encryption properties, either side can only discover the common secret key, without disclosing the other non-common keys.

Peer Intermediaries for Key Establishment (PIKE) - PIKE [7] is a random key predistribution scheme. The basic idea of PIKE is to use sensor nodes as trusted intermediaries to establish shared keys. Each node shares a unique secret key with a set of nodes. In the case of 2 -Dimension, a node shares a unique secret with each of the O(*n*) nodes in the horizontal and vertical dimensions. Therefore, any pair of nodes can have a common secret with at least one intermediate node.

B. *Asymmetric Key Management*

Public Key / Private Key is used for encryption/ Decryption. Sender and receiver generate encryption and signature key pairs, submit certificate requests along with proof of identity to a Certificate authority and receive CA-Signed certificates, which they can then use to authenticate one another and exchange encrypted message. Following schemes uses Asymmetric Key Management.

Secure Routing Protocol (SRP) - SRP is a decentralized public key management protocol which employs (t, n) threshold cryptography. The system contains three types of nodes; client - normal users of the network, server - responsible for generating partial certificates and storing certificates in a directory structure allowing client nodes to request for the certificates of other nodes and combiner nodes – responsible for combining the partial certificates into a valid certificate. The system also has an administrative authority – dealer, which has knowledge of the complete certificate signing key skCA. Every node in the network has a public/private key pair and it is the responsibility of the dealer to issue the initial certificate for the nodes public key as well as distributing the public key pkCA of the certificate authority which is needed to verify the certificates. The certificate authority as a whole has a public/private key pair, pkCA/skCA of which the public key is known to all network nodes. The private skCA, is shared among the server nodes according to Shamir's secret sharing scheme. It has no certificate revocation mechanism. Also it requires the server nodes store all of the certificates issued. This requires a synchronization mechanism that propagates any new certificates to all the servers. It also must handle the case when the network has been segmented and later rejoined.

Self-Organized Key Management (SOKM) - In this scheme[5] users' public and private keys are created by the users themselves. Certificates are stored and distributed by the nodes in a fully self organized manner. Each certificate is issued with a limited validity period. Certificate update routine allows used to update version of the existing certificate. Key authentication is performed via chains of public-key certificates. Each node maintains two local certificate repositories: the non updated certificate repository and the updated certificate repository. The non updated certificate repository of a node contains expired certificates that the node does not keep updated. The updated certificate repository of a node contains a subset of certificates that the node keeps updated. There are two types of certificate revocation: explicit and implicit. The issuer explicitly revokes a certificate by issuing a revocation statement and by sending it to the nodes who stored the certificate in question. The implicit revocation relies on the expiration time contained in the certificates. Every certificate whose expiration time passes is implicitly revoked. SOKM has great configuration flexibility and no need of boot strapping process. Web-of-trust relationship is used for certificate path and it is not strongly connected which is not suitable for ad-hoc network.

Secure and Efficient Key Management - SEKM [3] - Properties of this scheme are Decentralized key management scheme, Based upon virtual CA trust model, A group of servers is formed having partial system private key, This group collectively provides certificate service, Mesh formed between server nodes with aadvantages like No single point failure, Higher availability than centralized server approach and with ddisadvantages Off Line TTP required, No optimal value for threshold node t, Violation of symmetric relation between nodes, It does not break the routing – security independency cycle

Ubiquitous and Robust Access Control (URSA) - URSA is a localized key management scheme and based on threshold cryptography, all nodes are servers and are capable of producing a partial certificate. It has a distributed self-initialization phase that allows a newly joined node to obtain secret shares by contacting a coalition of *k* neighboring nodes without requiring the existence of an online secret share dealer. The basic idea is to extend the PSS technique by shuffling the partial shares instead of shuffling the secret sharing polynomials. The purpose of this shuffling process is to prevent deducing the original secret share from a resulting share. In URSA, every node should periodically update its certificate. To update its certificate, a node must contact its 1-hop neighbors, and request partial certificates from a collection of threshold *k* number of nodes. This will introduce either communication delays or cause search failures. It could potentially utilize services from 2-hop neighboring nodes. The advantage of this scheme is efficiency and secrecy of local communications, as well as system availability since the CA's functionality is distributed to all network nodes. On the other hand, it reduces system security, especially when nodes are not well-protected because an attacker can easily locate a secret holder without much searching and identifying effort. Also in a network where a node has a small number of neighbors and threshold *k* is much larger than the network degree *d*, a node that wants to have its certificate updated needs to move around in order to find enough partial certificates. Also it requires off line configuration before joining the network.

Mobile Certificate Authority (MOCA) - In MOCA certificate service is distributed to Mobile Certificate Authority (MOCA) nodes. Nodes which are physically more secure and computationally more powerful are chosen as MOCA nodes. In cases where nodes are equally equipped, they are selected randomly from the network. The trust model of this scheme is a decentralized model since the functionality of CA is distributed to a subset of nodes. A service-requesting node can locate $k + \alpha$ MOCA nodes either randomly, based on the shortest path, or according to the freshest path in its route cache. However, the critical question is how nodes can discover those paths securely since most secure routing protocols are based on the establishment of a key service in advance.

C. Group Key Management

Group key encrypts and protects all the messages flowing in a group of users. Only those who know the current group key are able to recover the original message. A group of multiple parties are formed and a common secret is agreed upon for secured exchange of messages. Group key agreement protocols helps to achieve better scalability, efficiency, and storage saving. It also needs to address the security issue related to membership changes. Entry or exit of any member from the group requires re – keying at periodic interval. Group key management protocols can be roughly classified into three categories, namely, centralized, decentralized, and distributed [13]. In centralized group key protocols, a single entity is employed to control the whole group and is responsible for re-keying and distributing group keys to group members. In the decentralized approaches, a set of group managers is responsible for managing the group as opposed to a single entity being held responsible. In the distributed method, group members themselves contribute to the formation of group keys and are equally responsible for the re-keying and distribution of group keys. However, group key management for large and dynamic groups in MANETs is a difficult problem because of the requirement of scalability and security under the restrictions of node's available resources and unpredictable mobility.

Simple and Efficient Group Key Management (SEGK) - Bing Wu, Jie Wu, and Yuhong Dong[2] proposed SEGK model in 2008. Two multicast tree are constructed in MANET for improving the efficiency and fault tolerances. One of the multicast trees is known as a blue tree and another multicast tree as a red tree. The connection of multicast tree is maintained by coordinator. Computation and distribution of intermediate keying materials to all member is done by group coordinator through the use of underlying tree links. To make the common group key each group member i.e. mobile node in MANET, participates in a share of a final common group key, which is updated periodically. This model presents the reliable double multicast tree formation and maintenance protocol, which ensures that it covers all group members. The initialization process is started by group coordinator with sending the join advertise message into the mobile ad-hoc network. No of mobile nodes are directly proportional to computation cost. The node can choose the red, blue and grey color according to the following situations:-If Total no of neighbors < Predefined Threshold Value, than node will chose the Grey Color. If probability = 0.5, than node will chose the Red or Blue Color. In SEGK model, any mobile node or group member can join and leave the network. To ensure the backward and forward security updating of group key is done very frequently. Two detection methods are described in SEGK model, (a) Tree Links, when the node mobility is not significant detection is done through tree links. (b) Periodic Flooding of Control Messages, for high mobility environment this method is used. This scheme is useful for collective and group oriented applications. But for very large and dynamic group applications, the operation degrades. Also it is not scalable.

Hybrid Key Management

Hybrid or composite keys are those key which are made from the combination of two or more than two keys and it may be symmetric or a asymmetric or the combination of symmetric & asymmetric key. Some of the important hybrid key management schemes are discussed here.

Cluster Based Composite Key Management - The nodes are grouped into clusters, and keys are distributed such that intra-cluster communication is secured using a symmetric cryptosystem and inter-cluster communication is secured using an asymmetric cryptosystem. Furthermore, threshold cryptography is used for distributed certificate handling. Mobile agents provide node revocation and PKG services in MANET. On the basis of current trust value and old public key, cluster head's public key is computed. Using the time stamp in key number key renewal process can be done easily. MA handles the role of key revocation process and the selection of PKG nodes. The solution provides a significant improvement in the performance of the key management solution in a highly hostile environment, and scales well to large networks. However, the formation of clusters is a difficult task[12].

Zone-Based Key Management Scheme - In this scheme [17]a zone is defined for each node and includes the nodes whose distance (e.g., in hops) is at most some predefined number. This distance is referred to here as the zone radius, r - zone. Each node use symmetric key management inside its zone and asymmetric key management used for inter-zone security, without depending on clustering. This scheme uses ZRP (Zone Routing Protocol).

Table 1 Comparative survey of Key management Schemes

	Reliability	Security	Scalability	Robustness
DKPS	Medium	Fair	Fair	Good
PIKE	Medium	Limited	Fair	Fair
SRP	Medium	Fair	Fair	Fair
SOKM	Medium	Fair	Fair	Good
SEKM	High	Good	Fair	Good
URSA	High	Fair	Fair	Good
MOCA	High	Good	Good	Good
ID Based	High	Good	Good	Fair
SEGK	Low	Poor	Good	Good

Identity Based Cryptosystem

The concept of identity-based crypto system was introduced by Shamir[14]. In these systems the public key is generated based on the identity of the node (e.g., email or IP address), and the private key is generated by a trusted third party called a private key generator (PKG). This cryptography method is called ID-based cryptography (IBC). It significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users' certificates. It also makes it much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components.

Shamir's Identity based Signature scheme[14]

Identity-based cryptography introduced by Shamir, removes the need for certificates. Identities are typically short — at least compared to certificates with a size of several kilobits. Assuming information that is by default transferred in the routing messages can be used as the public key, identity-based schemes may scale better than the traditional certificate-based approaches. This makes identity-based protocols interesting for bandwidth-limited ad hoc networks.

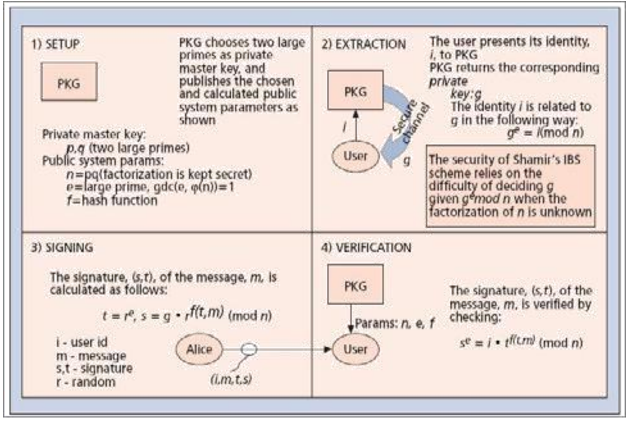
1) SETUP
PKG
PKG chooses two large primes as private master key, and publishes the chosen and calculated public system parameters as shown
Private master key:
p,q (two large primes)
Public system params:
n=pq(factorization is kept secret)
e=large prime, gdc(e, φ(n))=1
f=hash function
2) EXTRACTION
PKG
i
User
Secure channel
g
The user presents its identity, i, to PKG
PKG returns the corresponding private key:g
The identity i is related to g in the following way:
$g^e = i(\text{mod } n)$
The security of Shamir's IBS scheme relies on the difficulty of deciding g given g^emod n when the factorization of n is unknown
3) SIGNING
The signature, (s,t), of the message, m, is calculated as follows:
$t = r^e,\ s = g \cdot r^{f(t,m)}$ (mod n)
i - user id
m - message
s,t - signature
r - random
Alice
(i,m,t,s)
4) VERIFICATION
PKG
Params: n, e, f
User
The signature, (s,t), of the message, m, is verified by checking:
$s^e = i \cdot t^{f(t,m)}$ (mod n)

Figure 3 Shamir's Identity Based Signature Scheme Shamir constructed an identity-based signature (IBS) scheme. To verify a signature, it is enough to know the ID of the sender plus the public system parameters. The public system parameters are defined by the private key generator (PKG) during system set up. The public system parameters include the public key of the PKG and information about the message space. The PKG also generates the private signature keys corresponding to the user IDs. Figure 5 shows a sketch of Shamir's IBS scheme. During the setup phase, the PKG chooses a secret master key and generates the corresponding public system parameters. After wards, in the extraction phase, it issues private keys. The private keys are uniquely given by the IDs and the PKG private master key.

Boneh and Franklin's Identity based Encryption

Boneh and Franklin[4] introduced the first practical identity-based encryption scheme (IBE) . It is built from any bilinear map between two groups as long as a variant of the Computational Diffe-Hellman problem is hard. It uses the Weil pairing on elliptic curves as an example of such a map. It has following four steps:

Setup: takes a security parameter k and returns params (system parameters) and master-key. The system parameters include a description of a finite message space M, and a description of a finite cipher text space C. Intuitively, the system parameters will be publicly known, while the master-key will be known only to the "Private Key Generator" (PKG).

Extract: takes as input params, master-key, and an arbitrary and returns a private key d. Here ID is an arbitrary string that will be used as a public key, and d is the corresponding private decryption key. The Extract algorithm extracts a private key from the given public key.

Encrypt: takes as input params, ID, and M. It returns a cipher text C.

Decrypt: takes as input params, C, and a private key d. It return M.

These algorithms must satisfy the standard consistency constraint, namely when d is the private key generated by algorithm Extract when it is given ID as the public key, then For all M, Decrypt(params;C;d) = M where C = Encrypt (params; ID;M).

Advantages of Identity based cryptography

The main advantages of IBC are the simple key management process and reduced memory storage cost compared to traditional public key methods. Nodes must maintain only the PKG parameters, not the public key of all other nodes. In IBC every node is able to discover the public key of another node without exchanging any data. Moreover, a pair of nodes is able to compute a pair wise preshared key in a non interactive fashion. This preshared key can be used in authenticated encryption schemes and authenticated key agreement protocols.

Disadvantage of Identity base cryptography

The major problem with ID-based schemes is that the private key of all users must be known by the PKG. In conventional networks this is not an issue, but in MANETs in which the PKG must be distributed or emulated by an arbitrary entity, this might be a major issue. It also needs a safe channel to exchange private keys with each node. Also, ID-based schemes lack anonymity and privacy preservation, as public keys are directly derived from the identity of the nodes.

Identity based key management system

Identity based public key scheme: Identity-based public key schemes represent a new type of public key system. They allow user identities (e.g., e-mail or IP addresses) to be used as public keys, and make certificates superfluous. However, a trusted entity is required in order to generate and distribute the private keys corresponding to the various identities. The trusted entity is also needed for revocation. The trusted entity may sign a list of withdrawn identities. As with traditional public key systems, it has been suggested to spread the trusted entity over more nodes. Identity-based cryptography originated from the need to make key management easier and reduce the memory storage cost of conventional public key systems. Identity-based schemes are normally specified by four randomized algorithms

1. Setup: takes security parameters as input and returns a master public/private key pair for the system. The master private key is only known by the PKG.
2. Extract: takes the master private key and an identity of a node as input, and returns the personal private key of the node.
3. Encrypt: takes the master public key, the public key of the destination node (derived from its identity), and the message as input, and returns the corresponding cyphertext.
4. Decrypt: takes the master public key, the private key of the node, and a cyphertext as input and returns the decrypted message.

Several ID-based key management schemes can be found in the literature. This article presents the most important schemes for MANETs, discussing their approaches, strengths, and weaknesses.

1. Khalili-Katz-Arbaugh's Id based key management[11]

The key management scheme combines ID-based and threshold techniques. All n nodes that initialize the MANET form a distributed PKG set, called the threshold PKG. The threshold PKG has a master private key, which is distributed among these n nodes using a t-over-n scheme. This means that none of these nodes is able to reconstruct the master private key based on its own information. The master public key is distributed to all nodes of the network, including those joined later.

The public key of the nodes are their identities, while their private keys must be computed by the nodes of the threshold PKG. To receive its private key, a node presents its identity to atleast t nodes of the threshold PKG, and each of them sends a part of the private key back. Upon receiving t correct parts, the node builds its own private key.

The use of the threshold PKG, instead of the single PKG scheme, eliminates the single point of failure. To discover the private key of any user, an attacker must compromise at least t nodes. Honest nodes only need to contact t nodes in order to obtain their own private keys, making the scheme resilient to temporary loss of connectivity.

The scheme assumes that identities are recorded in hardware and cannot be altered. An attacker that creates false identities or alters its own identity can be a threat to it. Nodes that enter the network need a safe communication channel to at least t nodes of the threshold PKG to obtain their private keys. Furthermore, this scheme does not address key revocation or key renewing.

2.Deng-Mukharji-Agrawal's Id based key management[8]

The key management scheme has two components: distributed key generation and identity-based authentication. The key generation component provides the master key of the network and the public/private key pair for each node of the network. The identity- based authentication mechanism provides end-to-end authentication and confidentiality between nodes. If the authentication process succeeds, these nodes exchange a session key, which can be used for future communication.

The public/private master key is computed and distributed in the same fashion as in the Khalili-Katz-Arbaugh scheme. Hence, before using the network, each node must obtain its personal private key. To obtain the private key, a node must contact at least t nodes of the PKG, presenting its identity and requesting private key generation service. Each PKG node generates a secret part of the private key and sends it to the requesting node. Upon collecting t parts of the private key, the node can build its own private key and join the network. To ensure that the generated parts of the private key are securely transmitted, the requesting node must generate and present a temporary public key when sending the request. Each PKG node sends the generated part of the private key encrypted with this temporary public key. Like the Khalili-Katz -Arbaugh scheme, an attacker that creates false identities or alters its own identity might be a threat. Furthermore, this scheme does not address key revocation or renewal.

3. Identity based authentication and key exchange[9]

The identity-based authentication and key exchange (IDAKE) scheme consists of two techniques: a basic MANET-IDAKE and a fully self-organized MANET-IDAKE. IDAKE uses symmetric cryptography and pairing-based keys in both techniques, specified in six algorithms: setup, extract, distribute, compute shared key, key renewal, and key revocation.

The setup algorithm defines the long-term private and public keys of the PKG and announces the public key of the PKG to the network. The extract algorithm defines the long-term private key for the nodes of the network, recalling that their public key is their identity. The distribute algorithm bootstraps all nodes with their private keys. The compute shared key algorithm is invoked when nodes A and B want to communicate, computing a symmetric pairing based key that will be used in the communication. The key renewal algorithm is invoked when the key of a node expires or is revoked. The key revocation algorithm provides rules to revoke keys of compromised nodes, combining a neighbor watch with an accusation scheme. All these algorithms work in the same fashion in both basic and fully self-organized MANET-IDAKE.

Basic MANET-IDAKE consists of two phases: the initialization phase with access to an external PKG (setup, extract, and distribute algorithms) and the running system phase without access to a PKG (compute shared keys, key renewal, and key revocation algorithms). Note that the external PKG must initialize all devices before they join the network.

In fully self -organized MANET-IDAKE, all tasks are performed by the network nodes themselves, without any external PKG. The external PKG is emulated by the t-over-n threshold scheme like the previously presented schemes. However, the self-organized version does not specify how private keys are distributed to the nodes.

The MANET-IDAKE scheme has low bandwidth and low memory requirements due to the efficient key management of ID-based schemes. The MANET-IDAKE computational complexity depends on the implementation of the key revocation and renewal algorithms. The basic version of the scheme has a single point of failure, while in the distributed version this problem is eliminated.

4 Identity Based key management scheme (IKM)

Identity-based key management is a combination of ID-based key management and threshold cryptography. In IKM the public and private key of each node are composed by a node-specific ID-based element and a network wide common element. The node - specific element ensures that the secrecy of non-compromised nodes is not jeopardized even in the presence of several compromising nodes. On the other hand, the common element part enables very efficient network-wide public and private key updates via a single broadcast message. IKM has three phases: key predistribution, key revocation, and key update. The key predistribution occurs during network initialization, in which a PKG determines a set of system parameters and preloads every node with appropriate keying material. The PKG distributes its functionality to t distributed PKGs, called D-PKGs, selected among the nodes of the network. The private master key is distributed using a threshold t-over-n cryptography. This is done to enable secure and robust key revocation and update during network operation.

Key revocations must be explicit in order to minimize the damage from compromised nodes. During network operation,if any node suspects that another node is malicious or has been compromised, it sends a signed message to the DPKG. A node is considered bad when the number of accusations against it reaches a predefined value, called the revocation threshold. In IKM nodes must update their public/private keys in periodic intervals or when the number of revoked nodes reaches a predefined value. Revoked nodes cannot update their keys, thus becoming isolated from the network.

It is important to notice that an external PKG implies that if it is attacked, the entire network might be compromised. Also, the scheme is not resilient to temporary loss of connectivity. The Khalili-Katz-Arbaugh and Deng-Mukherjee-Agrawal schemes do not address key renewal for non-compromised nodes or key revocation of compromised ones. Furthermore, only Deng-Mukherjee-Agrawal specifies a way to distribute private keys after network formation or initialization and without a secure pre-established communication channel. All presented schemes use asymmetric keys. All these schemes have pros and cons, and their use depends on the user application.

Comparison of different Id based key management system

Figure 4 summarizes the main characteristics of the previously presented ID-based key management schemes.

Table 2 Comparison of ID Based Key management Schemes

	Khalili-Katz-Arbaugh	**Deng-Mukherjee-Agrawal**	**Bohio-Miri**	**Basic-IDAKE**
Threshold	Yes	Yes	No	Yes
PKG	Internal	Internal	External	External
Key Renewal	No	No	Yes	Yes
Key Revocation	No	No	Yes	Yes
Asymmetric keys	Yes	Yes	No	Yes
Private key distribution	Safe channel	Temporary key	Before net formation	Before net Formation

III. CONCLUSION

Security is an important feature that determines the success and degree of deployment of MANETs. Cryptography is a powerful tool to defend against a variety of attacks and helps to achieve a variety of security goals. Most cryptographic algorithms require the use of keying materials. If the cryptographic key is disclosed, then there is no security at all. Obviously, key management is in the central part of any secure communication and is the weakest point of the security. Various key management schemes for Mobile ad hoc networks are discussed and compared in this paper. The hybrid approach for key management is a promising research direction for scalable MANETs. More research efforts are sought in finding a more efficient way for creating the public key without losing the ability of creating certificates in a distributed manner. Designing and building an underlying secure, robust, and scalable key management system is a promising research area.

REFERENCES

[1] Anuraha Banerjee, “A Survey of multicast routing protocols for Mobile Ad Hoc Networks”, International International Journal of Engineering Science and Technology, vol.2 (10), 2010.

[2] Bing Wu, Jie Wu and YuhongDong,”An efficient group key management scheme for mobile ad hoc network”, International Journal and Networks, Vol. 2008.

[3] Bing Wu Et Al, “Secure and Efficient key Management in mobile ad hoc networks”, Network and Computer Applications, Vol. 30, pp. 937-954, 2007.

[4] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing, *Advances in Cryptology - CRYPTO `2001*, LNCS 2139, Springer Verlag, pp. 213-229, 2001.

[5] Capkun Et Al.: Self-organized Pulic-Key Management For Mobile Ad Hoc Networks, IEEE Transactions On Mobile Computing, VOL. 2, NO. 1, January-March 2003.

[6] Chan, A. (2004). “Distributed Symmetric Key Management for Mobile Ad hoc Networks”, *IEEE INFOCOM’04*, vol.4, pp. 2414- 2424

[7] Chan, H., Perrig, A., and Song, D. (2003). “Random Key Predistribution Schemes for Sensor Networks”. *IEEE Symposium on Security and Privacy* 2003. pp. 197- 213.

[8] H. Deng, A. Mukherjee, D.P. Agrawal. Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks, *International Conference on Information Technology: Coding and Computing (ITCC'04)*, vol. 1, pp. 107-115, 2004.

[9] K. Hoeper and G. Gong. Identity-Based Key Exchange Protocol for Ad Hoc Networks, *Canadian Workshop of Information Theory -CWIT `05*, pp. 127- 130, 2005.

[10] M. Ilyas. The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003

[11] A. Khalili, J. Katz, and W. Arbaugh. Toward Secure Key Distribution in Truly Ad-Hoc Networks, *2003 Symposium on Applications and the Internet Workshops (SAINT 2003)*, IEEE Computer Society, ISBN: 0-7695-1873-7, pp. 342-346, 2003.

[12] R. PushpaLakshmi, A. Vincent Antony Kumar,”Cluster Based Composite Key Management in Mobile Ad Hoc Networks”, International Journal of Computer Applications, vol. 4- No. 7, 2010

[13] Rafaeli, S. and Hutchison, D. (2003). A Survey of Key Management for Secure Group Communication. ACM computing Surveys, vol. 35, no. 3, pp. 309-329.

[14] A. Shamir. Identity-based Cryptosystems and Signature Schemes, *Advances in Cryptology- CRYPTO '84*, LNCS 196, Springer Verlag, pp. 47-53, 1984.

[15] Sunghee Woo, Topology-Based Multicast Routing Protocols for MANET, Journal of Next Generation Information Technology(JNIT) Volume 4, Number 8, October 2013

[16] Tanenbaum, A. (2003). Computer Networks, PH PTR.

[17] ThairKhdour, Abdullah Aref, “A Hybrid Schema Zone-Based Key Management For MANETS”, Journal of Theoritical and Applied Information Tecnology, vol. 35 No. 2, 2012.