iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Effective and Secure Key Management Schemes in MANETs-Review

A.D.Khamalakhannen[1], Suthanthira Vanitha[2]
Anna University, Chennai, Tamil Nadu, India

Abstract—In Mobile ad hoc network secure communication is challenging due to due to dynamic topology and mobility of nodes. For this reason, key management is particularly difficult to implement in such networks. Secure communication in a network is determined by the reliability of the key management scheme, which is responsible for generating, distributing and maintaining encryption/decryption keys among the nodes.
The purpose of key management is to provide secure procedures for handling cryptographic keying materials.
In MANETs, 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. A number of key management schemes have been proposed for MANETs.This paper presents generous various key management in MANET and also discussed about specific features and limitations of every protocol.
Keywords: key management, security, mobile ad hoc network.

I. INTRODUCTION

A. Mobile Ad Hoc Networks

A mobile ad-hoc network (MANET) [1] offers convenient infrastructure-free communication over the shared wireless medium. All the network functions are performed by nodes who behave as hosts as well as routers to enable direct communication with each other. Due to their self-organizing nature and because they do not require expensive fixed infrastructures, these networks have been found suitable for many applications. Evidently, these types of networks are vulnerable to security threats because of their dynamic topology [2]. Secure communication requires scalable and efficient membership management with appropriate access control measures to protect data and cope with potential compromises. MANETs don't have a fixed size: nodes can join or leave the network dynamically. When joining the network, nodes need
public and private keys (we assume the network has the computational ability to allow asymmetric cryptography). In absence of a central administration, key management must be self-organized by the nodes. Nodes obtain their keys with the help of other nodes, called master. Networks generally use a threshold scheme: a node must request at least t+1 master nodes out of n in order to obtain its key.

B. Characteristics Of Mobile Ad Hoc Networks

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to an interface with a fixed network. Its nodes are equipped with wireless transmitters/receivers using antennas that may be omni-directional (broadcast), highly directional (point-to-point), or some combination thereof. At a given time, the system can be viewed as a random graph due to the movement of the nodes and their transmitter/receiver coverage patterns, the transmission power levels, and the co-channel interference levels [3] [4] . The network topology may change with time as the nodes move or adjust their transmission and reception parameters. Thus, ad hoc networks have several salient characteristics:
Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology which is typically multihop and it may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate.
One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.
Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

C. Security Challenges Overview

1) Security Requirements: In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile adhoc network is very challenging. The goals to evaluate if mobile adhoc network is secure or not are as follows:
Security services include the functionality that is required to provide a secure networking environment. It comprises authentication, access control, confidentiality, integrity, nonrepudiation, and availability [5] [6] [7]. 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. The main security services can be summarized as follows:

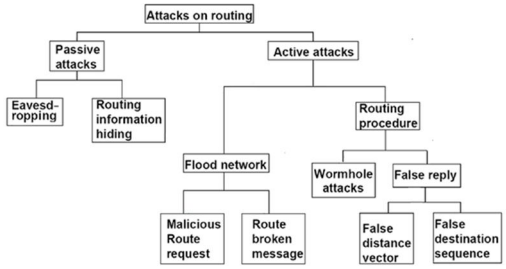
a) *Authentication:* The function of the authentication service is to verify a user's identity and to assure the recipient that the message is from the source that it claims to be from. First, at the time of communication initiation, the service assures that the two parties are authentic; that each is the entity it claims to be. Second, the service must assure that a third party does not interfere by impersonating one of the two legitimate parties for the purpose of authorized transmission and reception.
b) *Access control:* This service limits and controls the access of a resource such as a host system or application. To achieve this, a user trying to gain access to the resource is first identified (authenticated) and then the corresponding access rights are granted.
c) *Integrity:* The function of integrity control is to assure that the data is received exactly as sent by an authorized party. That is, the data received contains no modification, insertion, deletion, or replay.
d) *Confidentiality:* Confidentiality ensures that the data/information transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques such that only legitimate users can analyze and understand the transmission.
e) *Availability:* This involves making network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.
f) *Non-Repudiation:* This is related to the fact that if an entity sends a message, the entity cannot deny that it sent that message. If an entity gives a signature to the message, the entity cannot later deny that message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny the message with its signature.
g) *Anonymity:* Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

2) Security attacks: Securing wireless Adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two type's passive and active attacks. Many passive and active security attacks could be launched from the outside by malicious hosts or from the inside by Compromised hosts [8] [9] .While MANETs can be quickly and inexpensively setup as needed, security is a more critical issue compared to wired networks or other wireless counterparts.
a) Passive attacks: In passive attacks, an intruder captures the data without altering it. The attacker does not modify the data and does not inject additional traffic. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attacks are difficult to detect. A powerful encryption mechanism can alleviate these attacks, making it difficult to read the transmitted data.

b) Active attacks: In active attacks, an attacker actively participates in disrupting the normal operation of the network services. An attacker can create an active attack by modifying packets or by introducing false information. Active attacks can be further divided into internal and external.

c) Internal attacks: Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication. They are much more severe and difficult to detect compared to external attacks.

d) External attacks: External attacks are carried out by nodes that do not belong to the network. Such attacks are often prevented through firewalls or some authentication and encryption mechanisms.



The various attacks over the different layers in the Mobile Ad hoc Networks which are presented above are summarize in the Table1 according to their respective layer.

Table 1: Attacks on the Protocol Stack

Layer	Attack
Data Link Layer	Jamming attack
Network Layer	Blackhole attack, wormhole attack, Byzantine attack, sleep deprivation attack, state pollution attack, Sybil attack, modification and fabrication.
Transport Layer	SYN attack and Session Hijacking
Application Layer	Repudiation attack
Physical Layer	Evaesdropping,Jamming,Active interference

3) Security mechanisms: As we are aware of that MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets or impersonate a node. This violets the network's goal of availability, integrity, authentication and nonrepudiation. Compromised nodes can also launch attacks from within a network. Most proposed routing algorithms today do not specify schemes to protect against such attacks. We give below methods that are pertinent for authentication, key distribution, intrusion detection and rerouting in case of Byzantine failures in MANETs.

Cryptography is an important and powerful tool for secure communications. It transforms readable data (plaintext) into meaningless data (ciphertext). Cryptography has two dominant categories, namely symmetric-key (secret-key) and asymmetric-key (public-key) approaches [10].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. Although the asymmetric cryptography approaches are versatile (can be used for authentication, integrity, and privacy) and are simpler for key distribution than the symmetric approaches, symmetric-key algorithms are generally more computation-efficient than the asymmetric cryptographic algorithms [11]. 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. Meanwhile, the secret could be recovered by combining any threshold *k* pieces based on Lagrange interpolation. These cryptographic algorithms are the security primitives that are widely used in wired and wireless networks. They can also be used in MANETs and help to achieve the security in its unique network settings.

4) Key management: Key management is a central part of the security of MANETs. 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. In MANETs, 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. Some asymmetric and symmetric key management schemes (including group key) have been proposed to adapt to the environment of MANETs. Key management deals with key generation, key storage, distribution,updating, revocation, deleting, archiving, and using keying materials in accordance with security policies. In this article, we present a comprehensive survey of research work on key management in MANETs based on recent literature. This article is organized as follows: Section 1 gives an introduction of MANETs. Section 2 discusses key management and trust models in wired networks and MANETs. Section 3 presents the asymmetric key management schemes in MANETs. Section 4 presents the symmetric key management schemes in MANETs. The group key management schemes are shown in Section 5. In Section 6, we conclude the article and discuss possible future work.

II. FUNDAMENTALS OF KEY MANAGEMENT

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 [12] 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. In the Diffie-Hellman (DH) scheme [12], the communication parties at both sides exchange some public information and generate a session key on both ends. Several enhanced DH schemes have been invented to counter man-in-the-middle attacks. In addition, a multi-way challenge response protocol, such as Needham-Schroeder [13], can also be used. Kerberos [13], which is based on a variant of Needham-Schroeder, is an authentication protocol used in many real systems, including Microsoft Windows. However, in MANETs, the lack of a central control facility, the limited computing resources, dynamic network topology, and the difficulty of network synchronization all contribute to the complexity of key management protocols.

Key integrity and ownership should be protected from advanced key attacks. Digital signatures, hash functions, and the hash function based message authentication code (HMAC) [14] are techniques used for data authentication and/or integrity purposes. Similarly, the public key is protected by the public-key certificate, in which a trusted entity called the certification authority (CA) in PKI vouches for the binding of the public key with the owner's identity. In systems lacking a TTP, the public-key certificate is vouched for by peer nodes in a distributed manner,

such as pretty good privacy (PGP) [12]. In some distributed approaches, the system secret is distributed to a subset or all of the network hosts based on threshold cryptography. Obviously, a certificate cannot prove whether an entity is "good" or "bad". However, it can prove ownership of a key. Certificates are mainly used for key authentication.

A cryptographic key could be compromised or disclosed after a certain period of usage. Since the key should no longer be usable after its disclosure, some mechanism is required to enforce this rule. In PKI, this can be done implicitly or explicitly. The certificate contains the lifetime of validity - it is not useful after expiration. However, in some cases, the private key could be disclosed during the valid period, in which case the CA needs to revoke a certificate explicitly and notify the network by posting it onto the certificate revocation list (CRL) to prevent its usage.

Key management for large dynamic groups is a difficult problem because of scalability and security. Each time a new member is added or an old member is evicted from the group, the group key must be changed to ensure backward and forward security. Backward security means that new members cannot determine any past group key and discover the previous group communication messages. Forward security means that evicted members cannot determine any future group key and discover the subsequent group communication information. The group key
management should also be able to resist against colluded members.

III. OVERVIEW OF KEY MANAGEMENT SCHEMES IN MANETS

To achieve the high security in MANET different Key Management schemes are used. Using and managing keys for security is a crucial task in MANET due its energy constrained operations, limited physical security, variable capacity links and dynamic topology. In MANET speed varies depending upon the applications, for example, in commercial application (short range network) speed is high but in military application (long range network) speed is low, i.e. speed is inversely prepositional to network range. MANET have special features like network can work in standalone intranet as well as can be connected to large internet, it can cover the area bigger than a transmission range and by using internal routing can be rapidly deployable etc. Different cryptographic keys are used for encryption like symmetric key, public key, group key and hybrid key (symmetric key + asymmetric key). In symmetric key management same keys are used by sender and receiver. This key is used for encryption the data as well as for decryption the data. If n nodes wants to communicate in MANET k number of keys are required, where k = n (n-1)/2.
In public key cryptography, two keys are used one private key and another public key. Different keys are used for encryption and decryption. The private key is available only for individual and kept by source node and it is used for decryption. The public key is used for encryption and it available to the public. In each communication new pair of public and private key is created. It requires less no of keys as compared to symmetric key cryptography.
Asymmetric keys are used for short messages but symmetric keys are used for long messages If n nodes wants to communicate in MANET, k number of keys are needed, where k =2n.Group key in cryptography is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key is creating and distributing a secret for group members [15]. There are specifically three categories of group key protocol 1. Centralized, in which controlling and rekeying of group is being done by one entity. 2. Distributed, group members or a mobile node which comes in group are equally responsible for making the group key, distribute the group key and also for rekeying the group. 3. Decentralized, more than one entity is responsible for making, distributing and rekeying the group key.
Initialization of system users with in a network, generation, distribution, installation, control, revocation, destruction, storage, backup, archival, bootstrapping and maintenance of trust in keys are different services which are important for security of the networking system. 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. The study about the different types of key management schemes are given in this paper. Figure (1) shows the different existing key management schemes for MANET.

A. Asymmetric key management schemes

Recently, research papers have proposed different key management schemes for MANETs. Most of them are based on public-key cryptography. The basic idea is to distribute the CA's functionality to multiple nodes. Zhou and Hass [16] presented a secure key management scheme by employing *(t, n)* threshold cryptography. The system can tolerate t-1 compromised servers.Luo, Kong, and Zerfos [17] proposed a localized key management scheme in which all nodes are servers and the certificate service can be performed locally by a threshold number of neighboring nodes. Yi, Naldurg, and Kravets [18] put forward a similar scheme. The difference is that their certificate service is distributed to a subset of nodes, which are physically more secure and powerful than the others. Wu and Wu [19] also introduced a scheme that is similar to Yi, in which server nodes form a mesh structure and a ticket scheme is used for efficiency. Capkun,Buttyan, and Hubaux [20] considered a fully distributed scheme that is based on the same idea of PGP. Yi and Kravets [21] provided a composite trust model. Their idea was to take advantage of the positive aspects of both the central and fully distributed trust models.

B. Symmetric key management schemes

There are research papers that are based on the symmetric-key cryptography for securing MANETs. For instance, some symmetric key management schemes are proposed for sensor nodes that are assumed to be incapable of performing costly asymmetric

cryptographic computations. Pairwise keys can be preloaded into nodes, or based on the random key distribution in which a set of keys is preloaded. Chan [22] introduced a distributed symmetric key distribution scheme for MANETs. The basic idea is that each node is preloaded with a set of keys from a large key pool [23] [24]. 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. Chan and Perrig [25] introduced a symmetric key agreement scheme for the sensor nodes. The basic idea of their approach is that each node shares a unique key with a set of nodes vertically and horizontally (in 2-Dimensions).Therefore, any pair of nodes can rely on at least one intermediate node to establish the common key.

C. Group key management schemes

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 [26]. For instance, each time a new member is added or an old member is evicted from a group, the group key must be changed to ensure backward and forward security.

IV. ASYMMETRIC KEY MANAGEMENT SCHEMES IN MANETS

In asymmetric cryptography, two keys are required for each node. The recipient's public key, available to all the other nodes, is used by the transmitting node for encryption and his secret private key is used by the receiving node for decryption. Asymmetric key cryptography requires a fewer number of keys compared to symmetric key cryptography. More precisely, the number of keys is K=2*n, for n communicating nodes. In this section, we describe available asymmetric key cryptography schemes.

A. Secure routing protocol (SRP)

This scheme is composed of client nodes, server nodes, combiner node and an administrative authority that works as a dealer providing initial certificates to the MANET nodes. The client nodes are the normal users of the network while the server nodes are responsible of generating the partial certificates and storing the certificates in a directory. Finally, the combiner node combines the partial certificates from the servers into valid certificates [27].

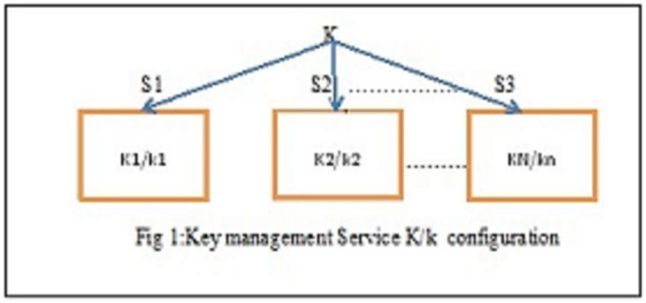


Fig 1:Key management Service K/k configuration

SRP is a decentralized public key management protocol proposed by Zhou and Hass [16] by employing *(t, n)* threshold cryptography [28] [29] [30] in their research paper called “Securing Ad Hoc Networks”. In the system, there are *n* servers, which are responsible for public-key certificate services. Therefore, the system can tolerate *t-1* compromised servers. Servers can proactively refresh the secret shares using the proactive secret sharing (PSS) [31] techniques or by adjusting the configuration structure based on share redistribution techniques to handle compromised servers or system failure. Since the new shares are independent of the old ones,mobile adversaries would have to compromise a threshold number of servers in a very short amount of time, which obviously increases the difficulty of the success of adversaries. The system configuration of this scheme is illustrated in Figure 1. The system public key K is distributed to all nodes in the network, whereas the private key S is split to *n* shares s1, s2, s3, …,sn, one share for each server according to a random polynomial function.

In this scheme, the system model is such that *n* servers are special nodes, each with its own public/private key pair and the public key of every node in the network. This is a critical issue in a large network. However, this scheme does not describe how a node can contact *t* servers securely and efficiently in case the servers are scattered in a large area. A share-refreshing scheme is proposed to counter mobile adversaries. The update of secret shares does not change the system public/private key pairs. Therefore, nodes in the network can still use the same system public key to verify a signed certificate so that the share-refreshing is transparent to all nodes. However, a method of distributing these updated subshares to all nodes securely and efficiently in the network is not addressed.

B. Ubiquitous and Robust Access Control (URSA)

URSA is a localized key management scheme proposed by Luo, Kong, and Zerfos [17] in their paper "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks". The URSA protocol is also based on threshold cryptography as in SRP [16]. The difference between URSA and SRP is that in URSA, all nodes are servers and are capable of producing a partial certificate, while in SRP only server nodes can produce certificates. Thus, certificate services are distributed to all nodes in the network. URSA also proposed 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. It can combine partial certificates into a legitimistic certificate. 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 attack can easily locate a secret holder without much searching and identifying effort. One problem is that in a sparse network where a node has a small number of neighbors, the threshold *k* is much larger than the network degree *d* and a node that wants to have its certificate updated needs to

move around in order to find enough partial certificate "producers". The second critical issue is the convergence in the share-updating phase. Another critical issue is that too great an amount of off-line configuration is required prior to accessing the networks.

C. Mobile Certificate Authority (MOCA)

The mobile nodes which having great computational power, physically more secure and on the basis of heterogeneity those mobile nodes used as MOCA nodes in this asymmetric key management scheme. MOCA is a decentralized key management scheme proposed by Yi, Naldurg, and Kravets [18] in their paper "Key management for heterogeneous ad hoc wireless networks". In this approach, a certificate service is distributed to Mobile Certificate Authority (MOCA) nodes. MOCA nodes are chosen based on heterogeneity if the nodes are physically more secure and computationally more powerful. 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 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.

D. Self-organized Key Management (SOKM)

Capkun, Buttyan, and Hubaux [20] considered a fully distributed key management scheme in their paper "Self-organized public key management for mobile ad hoc networks". This scheme is based on the web-of-trust model that is similar to PGP [12]. The basic idea is that each user acts as its own authority and issues public key certificates to other users. A user needs to maintain two local certificate repositories. One is called the non-updated certificate repository and the other one is called the updated certificate repository. The reason a node maintains a non-updated certificate repository is to provide a better estimate of the certificate graph. Key authentication is

performed via chains of public key certificates[32] that are obtained from other nodes through certificate exchanging, and are stored in local repositories.

In the self-organized network each mobile node public and private keys are generated by the nodes themselves, meaning that each node acts as a distinct CA. Each certificate has a validity period and the issuer of a certificate issues an update before its expiration. The node generates the update if it considers that the keying information in the certificate is correct. In this scheme, for a user to obtain another user's public key it acquires a chain of public key certificates. In this chain, the user can directly verify the first certificate, each one of the following certificates can be verified using the public key obtained from the previous To make sure the authentication certificate chain authentication process is correct, the node needs to check that all the certificates in the chain are

Volume 4 Issue III, March 2016
ISSN: 2321-9653

valid and correct [20].It has poor scalability and poor resource efficiency but having the off line authentication and limited intrusion detection security services. SOKS having high intermediates encryption operations and high storage cost [20].

The fully distributed, self-organized certificate chaining has the advantage of configuration flexibility and it does not require any bootstrapping of the system. However, this certificate chaining requires a certain period to populate the certificate graph. This procedure completely depends on the individual node's behavior and mobility. One the other hand, this fully self-organized scheme lacks any trusted security anchor in the trust structure that may limit its usage for applications where high security assurance is demanded. In addition, many certificates need to be generated and every node should collect and maintain an up-to-date certificate repository. The certificate graph, which is used to model this web-of-trust relationship, may not be strongly connected, especially in the mobile ad hoc scenario. In that case, nodes within one component may not be able to communicate with nodes in different components. Certificate conflicting is another potential problem in this scheme.

E. Composite Key Management

Recently, Yi, and Kravets [21] provided a composite key management scheme in their paper "Composite key management for ad hoc networks". In their scheme, they combine the centralized trust and the fully distributed certificate chaining trust models. This scheme takes advantage of the positive aspects of two different trust systems. The basic idea is to incorporate a TTP into the certificate graph. Here, the TTP is a virtual CA node that represents all nodes that comprise the virtual CA. Some authentication metrics, such as confidence value, are introduced in order to "glue" two trusted systems. A node certified by a CA is trusted with a higher confidence level. However, properly assigning confidence values is a challenging task.

F. Secure and Efficient Key Management (SEKM)

SEKM is a decentralized key management scheme proposed by Wu and Wu [15] [17] in their paper "Secure and efficient key management in mobile ad hoc networks". This is only one decentralized asymmetric key management scheme (based upon virtual CA trust model) which provides detailed, safe procedure for interacting, coordination between secret shareholders, and efficient that have more responsibility. All decentralized key management schemes are quite similar in that the functionality of the CA is distributed to a set of nodes based on the techniques of threshold cryptography. However, no schemes except for SEKM present detailed, efficient, and secure procedures for communications and cooperation between secret shareholders that have more responsibilities. In SEKM, all servers that have a partial system private key are to connect and form a server group. The structure of the server group is a mesh structure .Periodic beacons are used to maintain the connection of the group so servers can efficiently coordinate with each other for share updates and certificate service. The problem with SEKM is that, for a large network with highly dynamic mobility, maintaining the structure server group is very costly.

G. Identity-Based Key Asymmetric Management Scheme

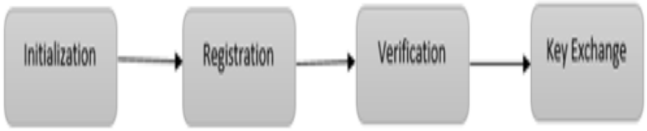


Figure: Identity-Based Key Asymmetric Management Scheme

In this scheme a trusted key generation center is needed. Generally this scheme consist four layers of key exchange process. Initialization, registration, verification and key Exchange. To verify the user identity and generating the corresponding private keys this scheme needs trusted key generation center. RSA scheme is used to construct the private-public key pair; each mobile node in MANET gets his long term public and private key pair. The secret key as a master key is chosen by key generation center randomly as well as publish its corresponding public key. In the initiation phase, each user receives his long term public and private key pairs by the generation center. The generation center randomly chooses a private key for ach node and publishes its corresponding public key. Next, the user registration phase where each users sends his ID to the generation center that provides him with his signature. In the user verification phase, users who wish to communicate challenge each other before generating the session keys in the key exchange phase after the security analysis of this model, it provides end-to-end authenticity and it prevents the network from brute force attack, man in a middle attack and from replay attack. Mobile nodes have no need to producing their public key and to

broadcast the keys in the network [33] - [35].

H. Partially Distributed Threshold CA Scheme (Z&H)

Partially Distributed Threshold CA Scheme was discovered by Zhou, L. and Hass, Z. in 1999. This scheme was founded by Zhou, L. and Hass, Z. in 1999. It uses the concept of trust distribution and threshold cryptography. Inside the network there are 'n' special nodes which is also called servers, each server maintains its own key pair and it is capable to store the public key of all the nodes including the servers in the network. This allows them to communicate securely with each other all the secure services like trust management, great intrusion tolerance and offline authentication are provided by CA (certification Authority). When the mobile ad-hoc network is constructed, this scheme is using the concept of CA distribution in threshold fashion. Security services like off line authentication, great intrusion tolerance, and trust management by CA (certification authority) are provided by Z&H asymmetric key management scheme. This scheme is working same as SEKM in which each and every server node produce a partial signature by using its private key. The only difference is this scheme is able to detect a compromised server in which combiner merges all the parts of the signature [36]. The survivability of resources efficiency is poor but it having the scalability of CRL (certificate revocation list), and certification.

I. Key Distribution Technique (ID-C)

In this scheme during the network formation each and every nodes produce a master public key in distributed manner. It is available to every node into the network a public key used for encryption which is produced by a master public key and individual node's ID. Similarly by combining the master private key and the nodes ID a node's private key is obtained.so in these approach nodes is using its IDs to generate keys. Set of mobile nodes creates or initialize the MANET with using the threshold private key generator identity based scheme. The generated key is accepted by self-organized network. Off net authentication, trust management and intrusion tolerances type security services are provided by ID-C asymmetric key management scheme. Scalability is provided through Id Revocation list with great resources efficiency. This scheme having medium intermediates, operation, encryption and storage cost [37].

J. Three Level Key Management Scheme

Secure and Highly Efficient Three Level Key Management scheme for MANET is proposed by Wan AnXiong, Yao Huan Gong in 2011. This scheme is based on threshold three level key management and identity- based scheme which adopts elliptic curve cryptography (ECC) and Bilinear pairing computation. In this scheme, when new node enters in MANET, its first task is to perform authentication operation with its neighboring nodes before all the nodes in the cluster can start a private key generation service(PKG), in which a new master public key is used in identity-based cryptosystem and a master private key is shared among the nodes. They all are in threshold (t-out-of-n) fashion. Means at least t number of nodes required to recover the new master secret key. Then the new node can acquire its corresponding personal private key by sharing their private keys from each of the t number of nodes which are forming PKG. new node acquires its personal public key by applying one way hash function and its own identity. Here, in this scheme bilinear map provides confidentiality and authentication with less computational cost and reduced communication overhead. Cryptography in order to achieve more efficiency and security [40, 41].

V. SYMMETRIC KEY MANAGEMENT SCHEMES IN MANETS

A. Distributed Key Pre-distribution Scheme (DKPS)

DKPS is a distributed symmetric key management scheme proposed by Chan [22] in the paper "Distributed symmetric key management for mobile ad hoc networks". It 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. 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.DKPS basically consist of three important phases 1. Distributed Key Selection (DKS): In the first phase every node takes the random key from the universal set in a way that satisfies the probability property Cover Free Family (CFF) concept is using for evaluating the exclusion property, to make a CFF in distributed manner probabilistic method is used. This technique removes the need of TTP (trusted third party) and makes the MANET more dynamic. 2.

Secure Shared-key Discovery (SSD): This is second phase of DKPS in which every node having a shared key with another node. Node can't found that which key in the ring are in common with which node. The trivial method is used for SSD.This method is not providing security but easy to evaluate because eavesdropping can occur in DKS phase.3. Key Exclusion Property Testing (KEPT):- Last phase of DKPS symmetric key management scheme is KEPT. Incidence matrix is used for present the relationship between mobile nodes key and shared keys it using binary values for constructing the matrix. KEPT phase test that is all keys of mobile nodes fulfilling the exclusion property of CFF. Features of DKPS are no need of TTP. DKPS needs less storage as compared to pair-wise key agreement approach. This scheme is more efficient as compared to group key agreement [22].

B. Peer Intermediaries for Key Establishment (PIKE)

PIKE is another symmetric key management scheme proposed by Chan and Perrig [25] in their paper "PIKE: Peer intermediaries for key establishment in sensor networks". It is a random key pre-distribution 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. This key pre-distribution scheme can be extended to three or more dimensions.

VI. GROUP KEY MANAGEMENT

The messages are protected by encryption using the chosen key, which in the context of group communication is called the group key. Only those who know the current group key are able to recover the original message. Group key establishment means that multiple parties want to create a common secret to be used in the secure exchange of information. Two people who did not previously share a common secret can create one common secret with a DH key exchange protocol. The 2-party DH protocol can be extended to a generalized version of the *n*-party DH

Key-exchange model. Research efforts have been put into the design of group key agreement protocols to achieve better scalability, efficiency, and storage saving, such as the introduction of a tree structure and hash function. Furthermore, the group key management also needs to address the security issue related to membership changes. The modification of membership could require the group key to be refreshed (e.g., periodic re-key). The change of group keys when old members leave or new members join ensures backward and forward security. Therefore, a group key scheme must provide a scalable and efficient mechanism to re-key the group.

Group key management protocols can be roughly classified into three categories, namely, centralized, decentralized, and distributed [26]. 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. Recently, collaborative and group oriented applications in MANETs have become an active research area. Obviously, group key management is a central building block in securing group communications in MANETs.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 nodes available resources and unpredictable mobility.

The literature presents several approaches to group key management. In this section, we give an overview of those protocols. Most of the following group key protocols are designed for the infrastructure networks. However, with the proper extension, some of them could be utilized and adapted to the MANET environment, or could serve as a hint for the design of MANET-specific group key management protocols. For instance, GDH (Section 5.4) and LKH (Section 5.1) have been extended into the MANETs. [42] proposed a simple and efficient group key management scheme, called SEGK, for MANETs. The basic idea of SEGK is that a physical multicast tree is formed in MANETs for efficiency. Group members take turns acting as group coordinator to compute and distribute intermediate key materials to group members. The keying materials are delivered through the tree links. The coordinator is also responsible for maintaining the connection of the multicast group. All group members can compute the group key locally in a distributed manner.

A. Simple and Efficient Group Key Management (SEGK)

In SEGK, every group member contributes to the formation of the common group key. This key can either be refreshed periodically

or only when the group members change. Bing Wu, Jie Wu, and Yuhong Dong were disclosed the SEGK model in 2008. Two multicast tree are constructed in MANET for improving the efficiency and maintains it in a parallel fashion to achieve the fault tolerances. SEGK model calls one multicast tree 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 intermediates keying materials to all member is does by group coordinator through the use of underlying tree links. To makes 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 start by group coordinator with sending the join advertise message into the mobile ad-hoc network. No of mobile nodes are directly propositional 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 [15].

VII. HYBRID OR COMPOSITE KEY MANAGEMENT SCHEMES IN MANET

Hybrid or composite keys are a combination of two or more symmetric, asymmetric, or symmetric and asymmetric keys. These schemes need to set two keys instead of one, which can present a problem for MANETs.

A. Cluster Based Composite Key Management

This model is disclosed by R.PushpaLakshmi and A. Vincent Antony Kumar in 2010. This scheme takes the concept of off-line CA, mobile agent, hierarchical clustering and partial distributes key management.

In this scheme, the network is divided into clusters and a cluster head, which is the node with the maximum trust ability and is selected by network administrator for each cluster. Moreover, *k* nodes with high trust value are selected in each cluster as Public Key Generation (PKG) nodes. Each node is assigned an ID by a CA prior to joining the network and has a self-assigned public key. The mobile agent collects node information and provides certificate revocation. A new node joining the network registers its information in the cluster head and the PKG nodes generate its private key shares. The shares are combined by the cluster head. The public key of the

cluster head is available to all the nodes in the cluster. The system uses a low frequency for communication between cluster members and a high frequency for communication between cluster heads [18].

B. Zone-Based Key Management Scheme

This key management scheme is based on the Zone Routing Protocol [44,45]. This model is proposed by ThairKhdour and Abdullah Aref in 2012, in this model for each mobile node zone is defined. Some pre-defined number is allocated to each mobile node which depends on the distance in hops. Symmetric key management is used by mobile node only for intra or inside zone radius. Without depends on clustering mobile node uses asymmetric key management for inter-zone security. It provides efficient way to making the public key without losing the capability of making the certificates [46].

VIII. CONCLUSION

The described key management schemes can be further classified into fully self-organized MANETs and authority based MANETs. The former do not have any online or offline authority while the later the trusted authority sets up the nodes before formation Of course, only the application can determine the suitable key management scheme to be used. It is obvious that group key can be very efficient since only one key pair needs to be generated but of course this scheme is more vulnerable and do not provide confidentiality between the different nodes.

Moreover, hybrid key management schemes seem to be more secure, compared to symmetric and asymmetric key management schemes, as they rely on two keys instead of one but require more operations associated with the generation and maintenance of the keys. As discussed previously, increasing the security of the network has a cost such as increased memory or increased power consumption, which is not always possible in MANETs.

ID based cryptography is very interesting since it provides a simple way to generate public and private key pairs. When this scheme is combined with threshold cryptography, it can provide an efficient way to generate keying material, prevent from man in the middle attacks as well as detect and identify cheaters in the group key protocol.

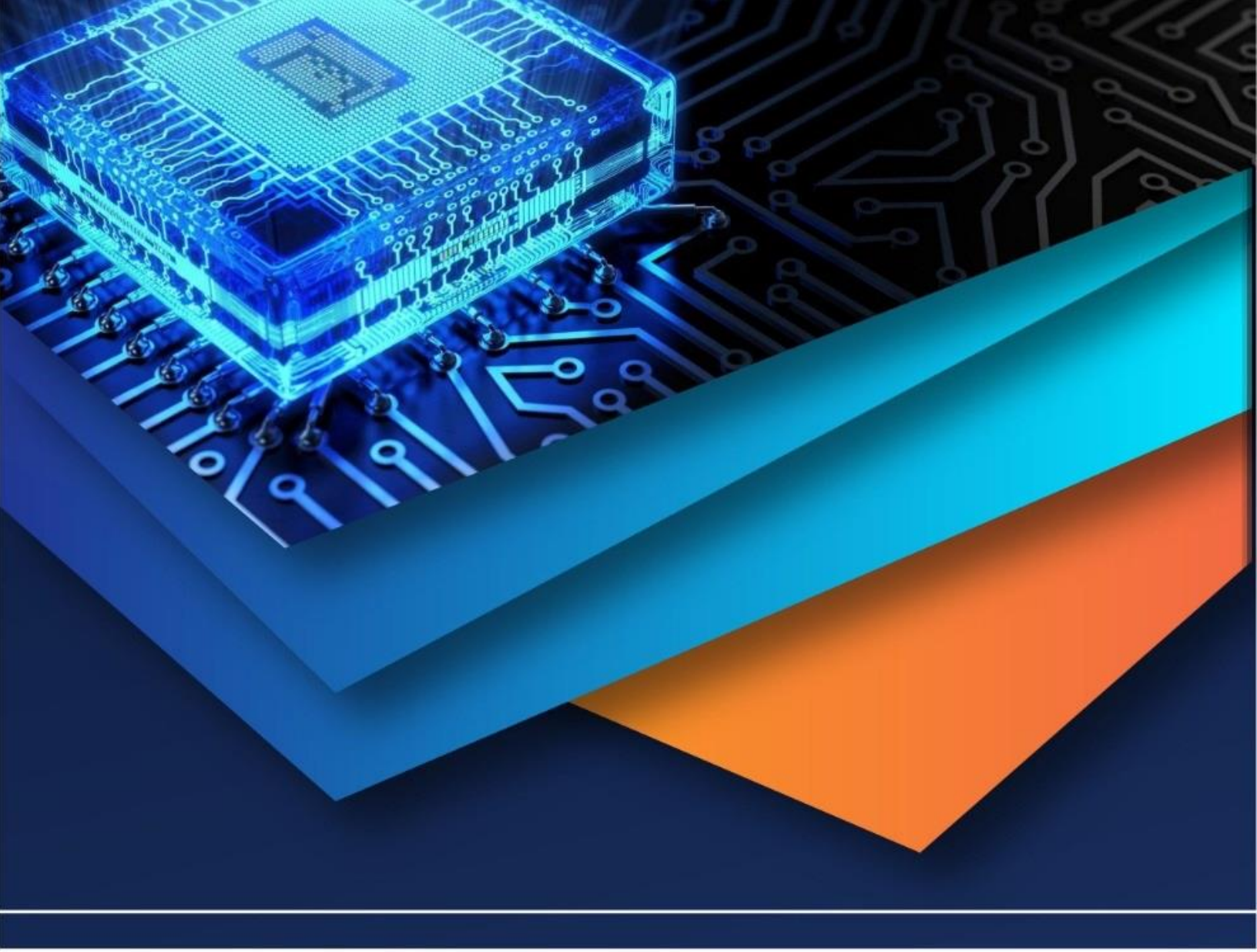
In summary, based on different assumptions, many key management protocols have been proposed for M\ANETs. All key management approaches are subject to various restrictions such as the mobile device's available resources, the network bandwidth, and MANETs dynamic nature. An efficient key management protocol for MANETs is an ongoing hot research area.

Analysis developed in this paper concerning the Key Management Schemes in M\ANET can be the basis of the area of future development of M\ANET Security as the exploration of new ideas on the exiting and elected schemes in the present paper or the development of new Key Management Schemes. The proposed scheme have to solve in accordance of its environment the dilemma to be at the optimum, simple to apply, formed on the fly, never expose or distribute key material to unauthorized nodes, assure system security does not succumb to compromised nodes, easily allow rekeying/key updates, enable withdrawal of keys when nodes are compromised or keys for other reasons should be revoked, be robust to Byzantine behavior and faulty nodes, work equally good no matter network size and number of neighbor nodes and efficiently handle network splits and joins.

REFERENCES

[1] Perkins, C. (2001). Ad Hoc Networks, Addison-Wesley.
[2] R. Sheikh, C. M. Singh and D. K. Mishra, Security issues in MANET:A review in Proc. WOCN, Sep. 2010.
[3] Stallings, W. (2002). Wireless Communication and Networks, Pearson Education.
[4] Ravi, S., Raghunathan, A., and Potlapally, N. (2002). Secure Wireless Data: System ArchitectureChallenges. Proc. of International Conference on System Synthesis.
[5] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. (2004). Security in Mobile Ad Hoc Networks:Challenges and Solutions. IEEE Wireless Communications, pp. 38- 47.
[6] Wu, B., Wu, J., Fernandez, E., Magliveras, S., and Ilyas, M. (2005). Secure and Efficient KeyManagement in Mobile Ad Hoc Networks. Proc. of 19th IEEE International Parallel & Distributed Processing Symposium, Denver.
[7] Nichols, R. and Lekkas, P. (2002). Wireless Security-Models, Threats, and Solutions, McGraw Hill,Chapter 7.
[8] Lou, W. and Fang, Y. (2003). A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. Ad Hoc Wireless Networks, edited by X. Chen, X. Huang and D. Du.Kluwer Academic Publishers, pp. 319-364.
[9] Murthy, C. and Manoj, B. (2005). Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR.
[10] Saloma, A. (1996). Public-Key Cryptography, Springer-Verlag.
[11] Tanenbaum, A. (2003). Computer Networks, PH PTR.
[12] Burnett, S. and Paine, S. (2001). RSA Security's Official Guide to Cryptography, RSA Press.
[13] Tanenbaum, A. (2002). Network Security, Chapter 8, Computer Networks. Prentice Hall PTR, 4thEdition.
[14] Menezes, A., Oorschot, P., and Vanstone, S. (1996). Handbook of Applied Cryptography, CRC Press.
[15] Bing Wu, Jie Wu and YuhongDong,"An efficient group key management scheme for mobile ad hoc network", International Journal and Networks, Vol. 2008.
[16] Zhou, L. and Haas, Z. (1999). Securing Ad Hoc Networks, IEEE Network Magazine vol.13, no. 6, pp.24-30.
[17] Luo, H., Zerfos, P., Kong, J., Lu, S., and Zhang, L. (2001). Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks. Proceeding of The 9th International Conference on Network Protocols.
[18] Yi, S., Naldurg, P., and Kravets, R. (2002). Security Aware Ad Hoc Routing for Wireless Networks Report No.UIUCDCS-R-2002-2290, UIUC.
[19] Wu, B., Wu, J., Fernandez, E., Magliveras, S., and Ilyas, M. (2005). Secure and Efficient Key Management in Mobile Ad Hoc Networks. Proc. of 19th IEEE International Parallel & Distributed Processing Symposium, Denver.
[20] Capkun, S., Buttya, L., and Hubaux, P. (2003). Self-Organized Public Key Management for Mobile Ad Hoc Networks, IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64.
[21] Yi, S. and Kravets, R. (2004). Composite Key Management for Ad Hoc Networks. Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61.
[22] Chan, A. (2004). Distributed Symmetric Key Management for Mobile Ad hoc Networks, IEEE INFOCOM.
[23] Chan, H., Perrig, A., and Song, D. (2003). Random Key Pre-distribution Schemes for Sensor Networks. To appear in Proc. of the IEEE Security and Privacy Symposium.
[24] Du, W., Deng, J., Han, Y., and Varshney, P. (2003). A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In Proc. of 10th ACM Conference on Computer and Communications Security (CCS), Washington DC.
[25] Chan, H. and Perrig, A. (2005). PIKE: Peer Intermediaries for Key Establishment in Sensor Networks, In Proceedings of IEEE INFOCOM.
[26] 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.
[27] C. Haowen and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks" in Proc. INFOCOM, 2005.
[28] Shamir, A. (1979). How to Share a Secret. Communications ACM 1979; 22(11), pp. 612–613.
[29] Wong, T., Wang, C., and Wing, J. (2002). Verifiable Secret Redistribution for Threshold Sharing Schemes. Technical Report, CMU-CS-02-114-R, School of Computer Science, Carnegie Mellon University.
[30] Stadler, M. (1996). Publicly Verifiable Secret Sharing. Proceeding of Eurocrypt'96. pp. 190-199.
[31] Herzberg, A., Jarecki, S., Krawczyk, H., and Yung, H. (1995). Proactive Secret Sharing or: How to Cope With Perpetual Leakage. Proceedings of Crypto'95,

vol. 5, pp. 339–52.
[32] del Valle, Gerardo, and Roberto Gómez Cárdenas. "Overview the key management in ad hoc networks."Advanced Distributed Systems. Springer Berlin Heidelberg, 2005. 397-406.
[33] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.
[34] Han, Kyusuk, et al. "A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication." International Journal of Communication Systems 24.4 (2011): 461-472.
[35] Kapil, Anil, and Sanjeev Rana. "Identity-Based Key Management in MANETs using Public Key Cryptography."International Journal of Security (IJS) 3.1 (2009): 1-26.
[36] Zhou, Lidong, and Zygmunt J. Haas. "Securing ad hoc networks." Network, IEEE 13.6 (1999): 24-30.
[37] Han, Kyusuk, et al. "A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication." International Journal of Communication Systems 24.4 (2011): 461-472.
[38] Khalili, Aram, Jonathan Katz, and William Arbaugh. "Toward secure key distribution in truly ad-hoc networks."Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.
[39] Xiong, Wan An, and Yao Huan Gong. "Secure and highly efficient three level key management scheme for MANET." WSEAS Trans. Comput 10.1 (2011): 6-15.
[40] Okamoto, Tatsuaki. "Cryptography based on bilinear maps." Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Springer Berlin Heidelberg, 2006. 35-50.
[41] Wu, B. and Wu, J. (2007). An Efficient Group Key Management Scheme for Mobile Ad HocNetworks. Accepted to appear in International Journal of Security and Networks (IJSN).
[42] 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.
[43] Balasubramanian A., Misha, S., Sridhar, R., "A Hybrid approach to key management for enhanced security in ad hoc networks", Technical report, university at Buffalo, NY, USA,2004.
[44] Balasubramanian A., Misha, S., Sridhar, R., "Analysis of a hybrid key management solution forad hoc networks IEEE WCNC'05, vol. 4, PP. 2082- 2087, 2005.
[45] ThairKhdour, Abdullah Aref, "A HYBRID SCHEMA ZONE-BASED KEY MANAGEMENT FOR MANETS", Journal of Theoritical and Applied Information Tecnology, vol. 35 No. 2,2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY