iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1258

www.ijraset.com

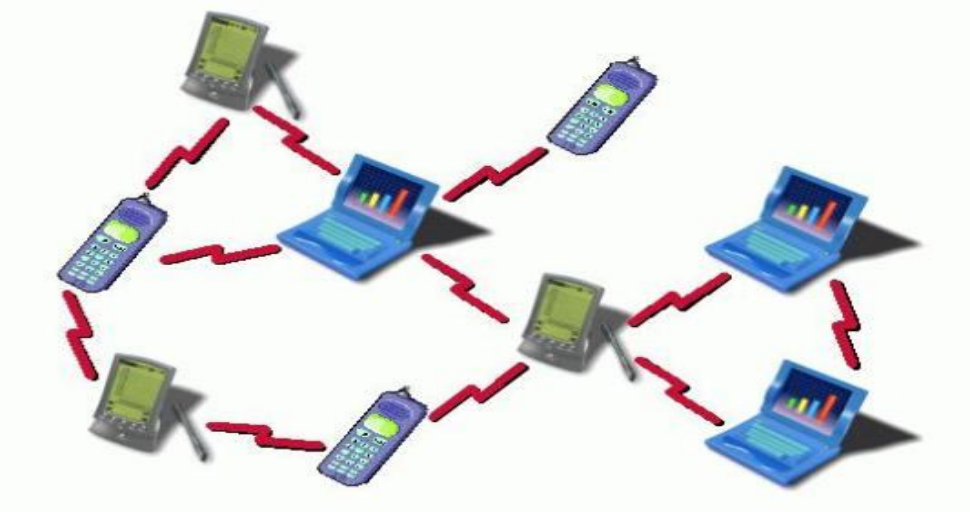
Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Key Management Schemes in MANET: A Review

Taranpreet Kaur[1]
[1]*Dept: Computer Science Mata Gujri College, Sri Fatehgarh Sahib*

Abstract: ***It is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its routable network properties where each node act as a "router" to forward the traffic to other specified node in the network.Cryptography is one of basis of security solutions for mobile ad hoc networks. Among public key techniques, the identity-based ones are very attractive for mobile environment, mainly due to their simple key management process and reduced memory storage costDifferent trust schemes are used to provide confidentiality, integrity and availability in mobile ad-hoc network to gain the secure environment .This paper, present the study on various kinds of key management schemes with their special features.***
Keywords: Mobile Ad-hoc Network, Identity based Cryptography, Key Management



I. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs are a kind of wireless ad hoc network (WANET) that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz) the growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc. 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.Mobile Ad-hoc Networks using Distributed Public- key Cryptography in pairing with Mobile Ad hoc Networks and various protocols are essential for secure communications in open and distributed environment. 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. There are specifically three categories of group key protocol 1. Centralized, inwhich 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.

A. Types of MANET

There are different types of MANETs including:

1) *In VANETs:* Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
2) *Vehicular ad hoc networks (VANETs)* : Enables effective communication with another vehicle or helps to communicate with roadside equipments.
3) *Internet Based Mobile Ad hoc Networks (iMANET)* :helps to link fixed as well as mobile nodes.

B. Characteristics of MANET

1) In MANET, each node acts as both host and router. That is it is autonomous in behavior.
2) Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
3) Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
4) The nodes can join or leave the network anytime, making the network topology dynamic in nature.
5) Mobile nodes are characterized with less memory, power and light weight features.
6) The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links.
7) All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
8) High user density and large level of user mobility.

C. The main security services can be summarized as follows

1) *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
2) *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.
3) *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.
4) *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.
5) *Availability:* This involves making network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.
6) *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.
7) *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.

D. Security Attacks

Securing wireless Ad-hoc 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 .While MANETs can be quickly and inexpensively setup as needed, security is a more critical issue compared to wired networks or other wireless counterparts.

1) *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.
2) *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.
3) *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.
4) *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 Black whole 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 Eavesdropping,Jamming,Active interference
5) *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 no repudiation. 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 (cipher text). Cryptography has two dominant categories, namely symmetric-key (secret-key) and asymmetric-key (public-key) approaches .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. 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.

E. 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, and 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.

F. 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 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, 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, can also be used. Kerberos, 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) 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). 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.

G. Overview Of Key Management Schemes In Manet

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. 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. 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 presented a secure key management scheme by employing (t, n) threshold cryptography. The system can tolerate t-1 compromised servers. Luo, Kong, and Zerfos 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 neighbouring nodes. Yi, Naldurg, and Kravets 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 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 considered a fully distributed scheme that is based on the same idea of PGP. Yi and Kravets provided a composite trust model. Their idea was to take advantage of the positive aspects of both the central and fully distributed trust models. 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 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. 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 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. 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. 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.

H. Asymmetric Key Management Schemes In Manet

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. 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. SRP is a decentralized public key management protocol proposed by Zhou and Hass by employing (t, n) threshold cryptography 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) 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 sub shares to all nodes securely and efficiently in the network is not addressed. Ubiquitous and Robust Access Control (URSA) URSA is a localized key management scheme proposed by Luo, Kong, and Zerfos 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. 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 neighbouring 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 neighbours, 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 neighbouring 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 neighbours, 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. 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 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. Self-organized Key Management (SOKM) Capkun, Buttyan, and Hubaux 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. 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 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 valid and correct .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. 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. Composite Key Management Recently, Yi, and Kravets 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. Secure and Efficient Key Management (SEKM) SEKM is a decentralized key management scheme proposed by Wu and Wu 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.

I. 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.

Cluster Based Composite Key Management this model is disclosed by R. Pushpa Lakshmi 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.

proposed by Their Khdour 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.

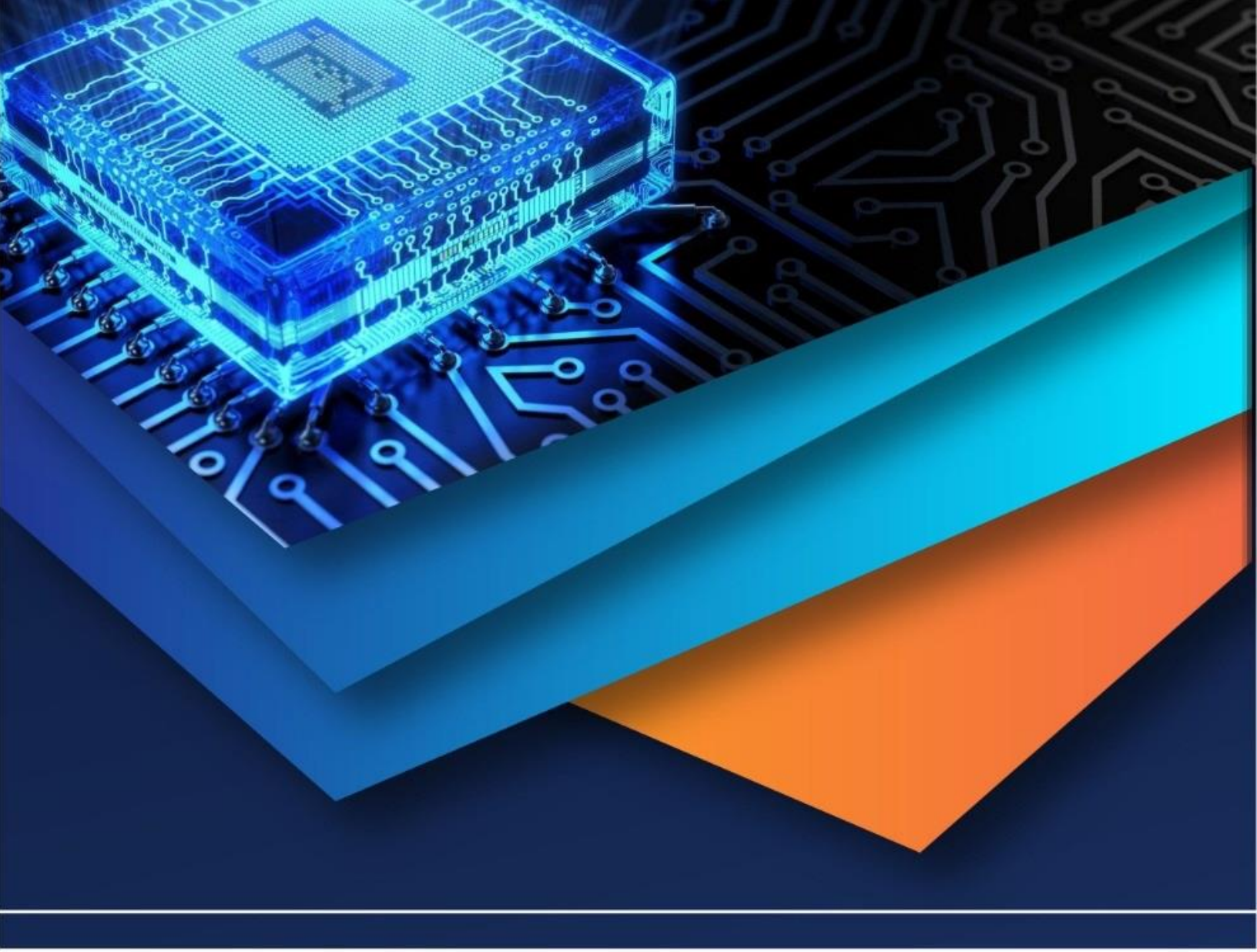
II. CONCLUSION

Different types of key management schemes are covered in this survey paper. In summary, 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. Cluster based & Zone based key schemes come in hybrid or composite key management scheme. In future work, we will focus in a particular key management scheme deeply and try to make a new key management scheme. Due to Features provided by MANETS, MANET attracts different real world application areas where the networks topology changes very quickly. 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.

REFERENCES

[1] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks."Communications Magazine, IEEE 40, no. 10 (2002): 70-75.
[2] Samba Sessay, Zongkai Yang and JianhuaHe ,"A Survey on Mobile Ad Hoc Wireless Network, " Information Technology Journal 3(2):168-175, 2004.
[3] Van der Merwe, J., Dawoud, D., and McDonald, " A survey on peer-to-peer key management for mobile ad hoc networks," ACM Comput. Surv. 39, 1, Article 1 , April 2007.
[4] Ms. Rajni1 , Ms. Reena2 "Review of MANETS Using Distributed Public-key Cryptography "International Journal of Computer Trends and Technology (IJCTT) – volume 10 number 3 – Apr 201
[5] Valle, G. and Cerdenas, R., "Overview the key Management in Ad Hoc Networks", ISSADS pp. 397 – 406, 2005.
[6] Luo, H. and Lu, S., "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", IEEE / ACM Transactions on Networking Vol. 12, pp. 1049-1063, 2004.
[7] RenuDalal,Yudhvir Singh and ManjuKhari "A Review on Key Management Schemes in MANET"International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012
[8] Wu, B., Wu, J., Fernandez, E., Ilyas, M. and Magliveras, S., "Secure and Efficient key Management in mobile ad hoc networks", Network and Computer Applications, Vol. 30, pp. 937-954, 2007.
[9] Zhou, L. and Hass, Z.,"Secure Ad Hoc Networks", IEEE Network Magazine vol. 13, no. 6, pp. 24-30, 1999.
[10] Capkun, S., Buttya, L., and Hubaux, P.,"Self-Organized Public Key Management for Mobile Ad Hoc Networks", IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, 2003.
[11] A. Khalili, Katz, Jonathan and Arbaugh, William A.," Towards secure key distribution in truly ad hoc networks", IEEE Workshop on Security and Assurance in ad hoc Networks – in conjunction with the 2003 International Symposium on Application and the Internet, 2003.
[12] AnilKapil and SanjeevRana, "Identity-Based Key Management in MANETs using Public Key Cryptography", International journal of Security, vol. (3): Issue (1).
[13] Wan AnXoing, Yao Huan Gong, "Secure and Highly Efficient Three Level Key Management Scheme for MANET", WSEAS TRANSACTIONS on COMPUTERS, Vol. 10, Issue 10, 2011.
[14] 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.
[15] 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.
[16] Balasubramanian A., Misha, S., Sridhar, R., "Analysis of a hybrid key management solution for ad hoc networks IEEE WCNC'05, vol. 4, PP. 2082- 2087, 2005.
[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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY