International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13 Issue 5, May, 2024, Impact Factor: 8.285

A Review Paper: Management Schemes in MANET

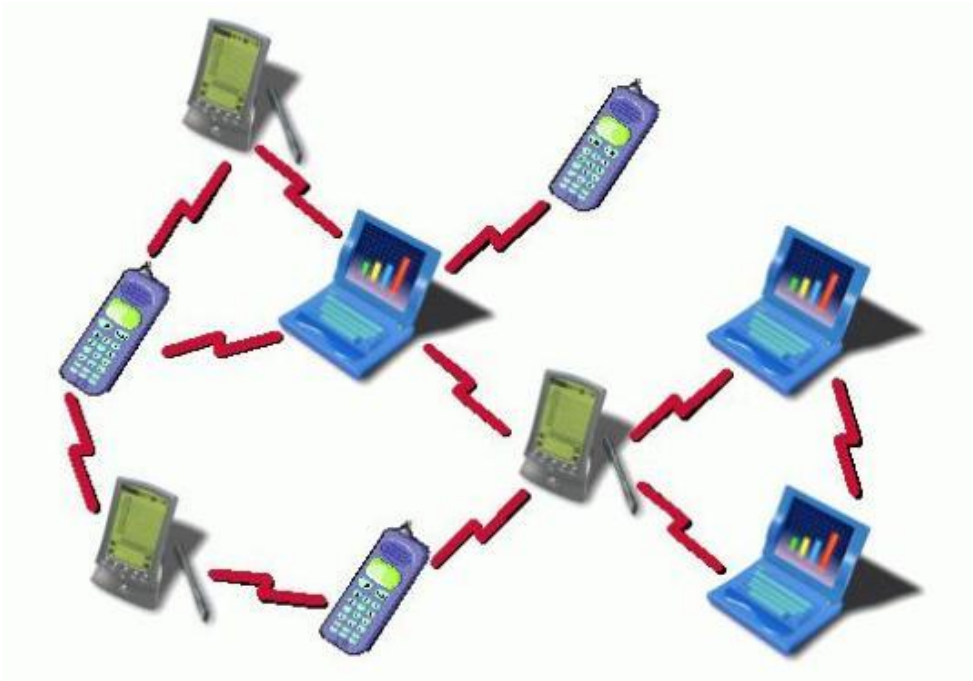
Taranpreet Kaur

Assistant Professor, PG Department of Computer Science, Mata Gujri College, Sri Fatehgarh Sahib

ABSTRACT

MANETs introduce a new communication which does not require fixed infrastructure.A mobile ad-hoc network (MANET) is based on a self-organizing and rapidly deployed networkit is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. MANET does not have a centralized administration mechanism. 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 cost.This paper; present the study on different kinds of management schemes with their special features.

Keywords: Mobile Ad-hoc Network, Identity based Cryptography, Management schemes



INTRODUCTION

A versatile adhocnetwork (MANET) may be a ceaselessly self-configuring, infrastructure-less arrange of versatile gadgets associated wirelessly. Each gadget in a MANET is free to move autonomously in any heading, and will in this manner alter its joins to other gadgets as often as possible. Each must forward traffic disconnected to its claim utilize, and thus be a switch. The essential challenge in building a MANET is preparing each gadget to ceaselessly keep up the data required to appropriately course activity. Such systems may work by themselves or may be associated to the bigger Web. They may contain one or numerous and diverse handsets between hubs. This comes about in a profoundly energetic, independent topology. MANETs are a kind of remote advertisement hoc arrange (WANET) that ordinarily encompasses a routable organizing environment on beat of a Connect Layer advertisement hoc arrange. MANETs comprise of a peer-to-peer, self-forming, self-healing organize. MANETs circa 2000-2015 regularly communicate at radio frequencies (30 MHz - 5 GHz) the development of tablets and 802.11/Wi-Fi remote organizing have made MANETs a well-known investigate subject since the mid-1990s. Numerous scholastic papers evaluate protocols and

their capacities, expecting shifting degrees of portability inside a bounded space, as a rule with all hubs inside a number of bounces of each other. Distinctive conventions are at that point assessed based on measures such as drop rate, the overhead presented by the steering convention, end-to-end parcel delays, arrange throughput, capacity to scale, etc. MANET have extraordinary highlights like organize can work in standalone intranet as well as can be associated to huge web, it can cover the region greater than a transmission extend and by utilizing inside directing can be quickly deployable etc. Portable Ad-hoc Systems utilizing Conveyed Open- key Cryptography in matching with Portable Advertisement hoc Systems and different conventions are fundamental for secure communications in open and conveyed environment. Distinctive cryptographic keys are utilized for encryption like symmetric key, open key, bunch key and crossover key (symmetric key + topsy-turvy key). In symmetric key administration same keys are utilized by sender and collector. This key is utilized for encryption the information as well as for unscrambling the information. On the off chance that n hubs needs to communicate in MANET k number of keys are required, where k = n (n-1)/2. There are particularly three categories of gather key convention 1. Centralized, in which controlling and rekeying of bunch is being done by one substance. 2. Conveyed, gather individuals or a versatile hub which comes in gather are similarly dependable for making the bunch key, convey the gather key conjointly for rekeying the bunch. 3. Decentralized, more than one substance is dependable for making, conveying and rekeying the bunch key.

Types of MANET

- InVANETs – Intelligent vehicular ad hoc systems make utilize of counterfeit insights to handle startling circumstances like vehicle collision.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Characteristics of MANET

• In MANET, each hub acts as switch. That's it is independent in behavior.
• Multi-hop radio transferring- When a source hub and goal hub for a message is out of the radio extend, the MANETs are competent of multi-hop steering.
• Conveyed nature of operation for security, directing and have arrangement. A centralized firewall is truant here.
• The hubs can connect or take off the arrange anytime, making the arrange topology energetic in nature.
• Portable hubs are characterized with less memory, control and light weight highlights.
• The unwavering quality, effectiveness, solidness and capacity of remote joins are frequently second rate when compared with wired joins.
• All hubs have indistinguishable highlights with comparable obligations and capabilities and subsequently it shapes a totally symmetric environment.
• Huge level of client portability.

The main security services can be summarized as follows:

a) Authentication: The work of the authentication is to confirm a user's character and to guarantee the beneficiary that the message is from the source that it claims to be from. To begin with, at the time of communication start, the benefit guarantees that the two parties are bona fide; that each is the substance it claims to be. Moment, the benefit must guarantee that a third party does not meddled by imitating one of the two authentic parties for the reason of authorized transmission and gathering.

b) Access control: This service limits and controls the access of a resource such as a host system or application. To realize this, a user attempting to pick up get to to the asset is to begin with distinguished (verified) and after that the comparing get to rights are allowed.

c) Integrity: The function of integrity control is to assure that the data is received exactly as sent by an authorized party. That’s, the information gotten contains no adjustment, inclusion, cancellation, or replay.

D) Privacy: Privacy guarantees that the data/information transmitted over the organize isn't uncovered to unauthorized clients. Privacy can be accomplished by utilizing diverse encryption methods such that as it were true blue clients can analyze and understand the transmission.

E) Accessibility: This includes making organize administrations or assets accessible to the authentic clients. It guarantees the survivability of the arrange in spite of malevolent rates.

f) Non-Repudiation: This is often related to the truth that in the event that a substance sends a message, the substance cannot deny that it sent that message. On the off chance that a substance gives a signature to the message, the substance cannot afterward deny that message. In open key cryptography, a hub A signs the message utilizing its private key. All other hubs can verify the marked message by utilizing A's open 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.

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.

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 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

Security mechanisms: As we are aware of that MANETs need central organization and earlier organization, so the security concerns are distinctive than those that exist in routine systems. Remote joins make MANETs more vulnerable to assaults. It is simpler for programmers to listen in and pick up get to to secret data. It is additionally simpler for them to enter or take off a remote organize since no physical association is required. They can moreover specifically assault the organize to erase messages, infuse untrue parcels or mimic a hub. This violets the network's objective of accessibility, keenness, verification and no disavowal. Compromised hubs can too dispatch assaults from inside a arrange. Most proposed routing calculations nowadays don't indicate plans to ensure against such assaults. We provide underneath strategies that are relevant for confirmation, key conveyance, interruption discovery and rerouting in case of Byzantine disappointments in MANETs. Cryptography is a critical and effective apparatus for secure communications. It changes clear information (plaintext) into aimless information (cipher content). Cryptography has two overwhelming categories, specifically symmetric-key (secret-key) and asymmetric-key (public-key) approaches .In symmetric-key cryptography, the same key is utilized to encrypt and unscramble the messages, whereas within the asymmetric-key approach, diverse keys are utilized to change over and recoup the data. In spite of the fact that the hilter kilter cryptography approaches are flexible (can be utilized for confirmation, keenness, and protection) and are less complex for key conveyance than the symmetric approaches, symmetric-key calculations are by and large more computation-efficient than the deviated cryptographic calculations. There are assortments of symmetric and hilter kilter calculations accessible, including DES, AES, Thought, RSA, and EIGamal. Limit cryptography is another cryptographic procedure that's very diverse from the over two approaches. In Shamir's (k, n) mystery sharing plot, mystery data is part into n pieces agreeing to an irregular polynomial. Meanwhile, the mystery might be recouped by combining any edge k pieces based on Lagrange addition. These cryptographic calculations are the security primitives that are broadly utilized in wired and wireless networks. They can moreover be utilized in MANETs and offer assistance to attain the security in its interesting organizes settings.

Overview of management schemes in MANET
To achieve the measures security in MANET distinctive Key Administration plans are utilized. Utilizing and managing keys for security could be a vital assignment in MANET due its vitality obliged operations, constrained physical security, variable capacity joins and energetic 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 keyin symmetric key administration same keys are utilized by sender and collector. This key is utilized for encryption the information as well as for unscrambling the information. In case n hubs needs to communicate in MANET k number of keys are required, where k = n (n-1)/2. In open key cryptography, two keys are utilized one private key and another open 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.

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 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.

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 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.

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. 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.

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.

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.

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.

b.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 wellprotected 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 shareupdating 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 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 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.

E.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.

F.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.

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.

b. Zone-Based Key Management Scheme This key management scheme is based on the Zone Routing Protocol. 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.

CONCLUSION

There are different types of 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 2014
[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]. Renu Dalal,Yudhvir Singh and Manju Khari "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
[18]. A. Rahman, "GRBF-NN based ambient aware realtime adaptive communication in DVB-S2," J Ambient Intell Human Comput., 2020.
[19]. F. Alhaidari, A. Rahman, and R. Zagrouba, "Cloud of Things: architecture, applications and challenges," J Ambient Intell Human Comput., 2020.
[20]. A. Rahman, S. Dash, and A. K. Luhach, "Dynamic MODCOD and power allocation in DVB-S2: A hybrid intelligent approach." Telecommun Syst, vol. 76, pp. 49–61, 2021.
[21]. M. Ahmad, M. A. Qadir, A. Rahman, et al., "Enhanced query processing over semantic cache for cloud based relational databases." J Ambient Intell Human Comput., 2020.