ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID SCHEMA ZONE-BASED KEY MANAGEMENT FOR MANETS

[1]Thair Khdour, [2]Abdullah Aref

[1]Asstt Prof., Department of Information Technology, Al-Balqa Applied University, Jordan

[2]Lecturer., College of Computer and Information Sciences, Princess Nora Bent Abdul Rahman University, Sudia Arabia

E-mail: [1]khdour@bau.edu.jo , [2]amaref@pnu.edu.sa

ABSTRACT

As various applications of wireless ad hoc network have been proposed, security has become one of the big research challenges and is receiving increasing attention Securing communications in resource constrained, infrastructure-less environments such as Mobile Ad Hoc Networks (MANETs) is very challenging. Cryptographic techniques are widely used for secure communications in wired and wireless networks. Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key management is weak. The purpose of key management is to provide secure procedures for handling cryptographic keying materials. The tasks of key management include key generation, key distribution, and key maintenance. 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. A number of key management schemes have been proposed for MANETs. In this paper, we present a survey of the research work on key management in MANETs according to recent literature then we propose a zone based variant of the recently proposed cluster-based hybrid schema, with an attempt to keep the advantages of the hybrid schema.

Keywords: *Mobile Ad Hoc Networks (MANETs), Key Management, Zone-Based Key Management, Hybrid Schema.*

1. INTRODUCTION

While in the past, there was a central mainframe computer with terminals for many users, currently there are one or more computers for each person. However, we are moving to the Ubiquitous Computing age, where one person will have multiple devices available in his or her environment (i.e., cell phones, laptops, handheld digital devices or personal digital assistants) and where computational power will be available everywhere [16]. The nature of ubiquitous computing and communication devices makes wireless networks a vital solution for their interaction. Hence, the wireless communication arena is growing to meet different challenges [8]. Undoubtedly, the most demanded service by mobile users is network connections and corresponding data services. Most of the existing connections among these wireless devices are infrastructure-based provided by service providers or private networks [8]. Base stations are used to connect wireless networks to the "outside" world. A mobile device inside a wireless network connects to the closest base station that is within its communication radius. As the mobile unit moves out of a base station's range into another's range, the mobile unit's connection is handed from the old base station to the new one, and the mobile device is able to continue communication as usual. Office Wireless Local Area Networks (WLANs) are typical applications of this type of network include providing the needed network services when the required networking infrastructures are not available in a given area is a real challenge[14]. Instead of relying on networking infrastructure, mobile devices may cooperate and provide the desired connectivity resulting in an ad hoc mobile network that is both flexible and powerful. This way, mobile nodes can communicate with each other and extend Internet services to an infrastructure-less area through the Internet gateway node [8]. Ad hoc mobile networks have no fixed routers; all nodes are capable of moving as well as of being connected dynamically in an arbitrary manner (as shown in Figure 1). Each node may act as a sender, a receiver and a router simultaneously [18]. Emergency search-and-rescue operations, conferencing, in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain are examples of ad hoc networks.

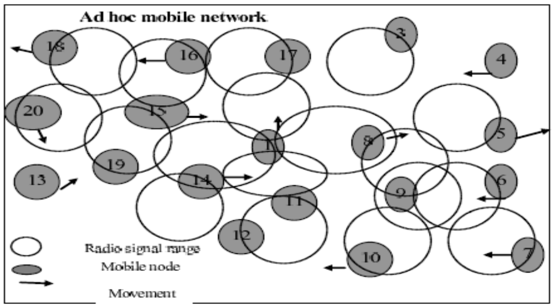

Figure. 1. MANET with Dynamic Mobile Nodes.

1.1 CHARACTERISTICS OF MANETS

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. 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. The network topology may change with time as the nodes move or adjust their transmission and reception parameters.

A mobile ad hoc network has several characteristics. Unlike the traditional mobile wireless networks that need base stations and access points to function properly, a mobile ad hoc network is infrastructure-less. As a result, in a MANET, network activities, including the discovery of the topology and delivery of messages, are executed by the nodes themselves.

Dynamic topology is another characteristic of a MANET. Nodes are able to move freely, causing the network topology to change rapidly and unpredictably over time. Multi-hop routes are automatically found using various routing mechanisms.

A MANET operates on bandwidth-constrained and variable-capacity links. Wireless links have lower capacity than hard-wired links. As such, a MANET has relatively low bandwidth links, high bit error rates, and unstable and asymmetric links. This is in contrast to wired networks, which are characterized by high bandwidth links, low bit error rates and stable and symmetric links. As a result, congestion often occurs.

Moreover, a MANET is often limited by energy-constrained operations. This is because some or all of the nodes in a MANET are battery-powered devices. Since the mobile nodes rely on this exhaustible method of energy, power conservation is important for optimization in a MANET system design.

Lastly, there is a limited physical security. Compared to hardwired networks, nodes of a MANET are subject to the physical security threats of eavesdropping, interception, denial-of-service and routing attacks. Hence, security techniques have to be applied to reduce these threats. Furthermore, the decentralized nature of a network control adds robustness against a single point of failure compared to centralized approaches [9]. Even though the need for scalability is not unique to MANETs, However, mechanisms required to achieve scalability in light of the preceding characteristics are not straightforward.

1.2 SECURITY

In this section we highlight different threats and attacks, security services and security mechanisms.

1.2.1 THREATS AND ATTACKS

While MANETs can be quickly and inexpensively setup as needed, security is a more critical issue compared to wired networks or other wireless counterparts. They are especially vulnerable to most kinds of already known attacks. Their distributed nature also enables completely new types of attacks (or makes known attacks much more effective). Many passive and active security attacks could be launched from the outside by malicious hosts or from the inside by compromised hosts. In passive attacks, an intruder captures the data without altering it. The attacker does not modify the data and does not inject additional traffic. In active attacks, an attacker actively participates in disrupting the normal operation of the network services. This section gives a brief summary of the different attack classes. It is not intended to give a complete listing but to show the principal threats ad hoc networks are facing and that very few malicious nodes can disable normal network operation.

Any participating node (insider) can spoof or alter routing information. The specific attack behaviors are related to the routing protocol used. For example, for some protocols, the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list. When distance-vector routing protocols are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes. By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even nonexistent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case [13].

In a Sybil attack a single node presents multiple identities to other nodes in the network or the attacker may further subvert existing nodes in the network, or fabricate its identity and impersonate another legitimate node [15].

Sinkhole Attacks typically works by making a malicious node looking especially attractive to surrounding nodes with respect to the routing algorithm. The goal is to absorb as much traffic as possible from a particular area through a compromised node, creating a sinkhole with the adversary at the center. This attack is especially effective in networks with a special communication pattern like sensor networks or surroundings of Internet gateways [15].

In Wormhole attacks an adversary tunnels messages from one part of the network usually via a low latency out of bound channel to another part of the network where they are replayed. These attacks can, among others, be used to distort routing, create sinkholes and to exploit routing race conditions as well as work even in the presence of authenticated and encrypted routing in [15].

HELLO flood attacks are applicable against all protocols that use HELLO messages to form neighborhood relationships among the nodes. A malicious node can send, record or replay HELLO messages into the network with high transmission power and therefore convince every node in the network that he is its neighbor. This attack leaves the network in confusion as most nodes simply send their packets into oblivion [15].

Malicious nodes can perform selective forwarding attack by dropping the packets, modifying the content of the packets, or duplicate the packets it has already forwarded messages instead of just forwarding them further along there paths. More complicated forms of this attack that make detection very hard, include the selective dropping of certain packets only. This attack works best if the attacker is directly included in the forwarding path. Malicious nodes can achieve this, especially, with routing protocols that utilize multiple routes to the destination [15].

Another type attacks is the denial-of-service (DoS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET [15].

1.2.2 SECURITY SERVICES

Cryptography may be used to perform several basic security services: confidentiality, data integrity, authentication, authorization and non-repudiation. These services may also be required to protect cryptographic keying material. In addition, there are other cryptographic and noncryptographic mechanisms that are used to support these security services. In general, a single cryptographic mechanism may provide more than one service (e.g., the use of digital signatures can provide integrity, authentication and non repudiation) but not all services. The main security services can be summarized as follows as described in [22]:

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.

Confidentiality: It 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.

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.

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.

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.

Availability: This involves making network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.

1.2.3 SECURITY MECHANISMS

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. 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 [19]. Threshold cryptography is another cryptographic technique that is quite different from the above two approaches where a secret is to be shared among a group of users (also called shareholders) in such a way that no single user can deduce the secret from his share alone. One classical (t, n) secret sharing algorithm was proposed by Adi Shamir in 1979, which is based on polynomial interpolation. In the scheme, the secret is distributed to n shareholders, and any t out of the n shareholders can reconstruct the secret, but any collection of less than t partial shares can not get any information about the secret [12]. However, most cryptosystems rely on the underlying secure, robust, and efficient key management subsystem. In fact, all cryptographic techniques will be ineffective if the key management is weak. Key management is a central part of the security of MANETs. 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.

2. KEY MANAGEMENT IN MANETS

As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As MANETs significantly vary from each other in many aspects, an environment-specific and efficient key management system is needed. Key is a piece of input information for cryptography algorithms, if the key is disposed so that, the encrypted information would be disclosed the security in networking depends, in many cases, on proper key management. Key management consists of various services, of which each is vital for the security of the networking systems. The services must provide solutions to be able to answer the following questions: Trust model, Cryptosystems, Key creation, Key storage and Key distribution [17].

The key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be distributed so that confidentiality, authenticity and integrity are not violated. For instance whenever symmetric keys are applied, both or all of the parties involved must receive the key securely. In public-key cryptography the key distribution mechanism must guarantee that private keys are delivered only to authorized parties. The distribution of public keys need not preserve confidentiality, but the integrity and authenticity of the keys must still be ensured. While some frameworks are based on a centralized trusted third party (TTP), others could be fully distributed. For example, a certification authority (CA) is the TTP in asymmetric cryptosystems, a key distribution center (KDC) is the TTP in the symmetric system, and in PGP no TTP is assumed. Because of the dynamic environment and the transient relationships among mobile nodes, the centralized approach is regarded as inappropriate for MANETs [19].

2.1 KEY MANAGEMENT SCHEMES IN MANETS

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. 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. Combining booth symmetric and asymmetric with the hope to bet the best of booth has also been proposed. 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. Group Key Management Schemes are out of the scope of this work, they are surveyed in [4].

2.2 ASYMMETRIC KEY MANAGEMENT SCHEMES IN MANETS

a) Secure Routing Protocol (SRP)

SRP is a decentralized public key management protocol proposed by Zhou and Hass\cite {Zhou} by employing (t, n) threshold cryptography. The system contains three types of nodes; client, server and combiner nodes. The client nodes are the normal users of the network while the server and combiner nodes are part of the certificate authority. The server nodes are responsible for generating partial certificates and storing certificates in a directory structure allowing client nodes to request for the certificates of other nodes. The combiner nodes which are also server nodes are responsible for combining the partial certificates into a valid certificate. The system also has an administrative authority which will be termed the dealer. The dealer is the only entity in the system that has knowledge of the complete certificate signing key skCA.

Every node in the network has a public/private key pair and it is the responsibility of the dealer to issue the initial certificate for the nodes public key as well as distributing the public key pkCA of the certificate authority which is needed to verify the certificates. The certificate authority as a whole has a public/private key pair, pkCA/skCA of which the public key is known to all network nodes. The private skCA, is shared among the server nodes according to Shamir's secret sharing scheme.

The solution has a number of faults or weaknesses of which the lack of a certificate revocation mechanism is the most critical. Any solution based on certificates should, considering the risk of compromise in ad hoc networks, provide such a mechanism. Also the solution requires that the server nodes store all of the certificates issued. This requires a synchronization mechanism that propagates any new certificates to all the servers. It also must handle the case when the network has been segmented and later rejoined [17].

b) Ubiquitous and Robust Access Control (URSA)

The URSA protocol uses a (k, n) threshold scheme to distribute an RSA certificate signing key to all nodes in the network. It also uses verifiable and proactive secret sharing mechanisms to protect against denial of service attacks and compromise of the certificate signing key. The capabilities of the CA are distributed to all nodes in the ad hoc network. Any operations requiring the CA's private key skCA can only be performed by a coalition of k or more nodes. The services provided by the CA can be grouped as certificate related services and system maintenance services.

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 [11].

The availability of the service is based on the assumption that every node will have a minimum of k one-hop neighbors and that the nodes are provided with a valid certificate prior to their joining the network. The system then provides services to maintain and update these initial certificates.

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. In a sparse network, where a node has a small number of neighbors, a node that wants to have its certificate updated needs to move around in order to find enough partial certificate, the convergence in the share-updating phase, great number of off-line configuration is required prior to accessing the networks [17].

c) Mobile Certificate Authority (MOCA)

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 [21]. 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)

The basic idea of this protocol 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 [5]. 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 [17].

e) Composite Key Management

This scheme combines the centralized trust and the fully distributed certificate chaining trust models. Composite Key Management 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 [20]. However, properly assigning confidence values is a challenging task.

f) Secure and Efficient Key Management (SEKM)

SEKM is a decentralized key management scheme based on the decentralized virtual CA trust model. 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 [19]. The problem with SEKM is that, for a large network with highly dynamic mobility, maintaining the structure server group can be costly.

2.3 SYMMETRIC KEY MANAGEMENT SCHEMES IN MANETS

a) Distributed Key Pre-distribution Scheme (DKPS)

DKPS is a distributed symmetric key scheme for MANETs is proposed in [6], where node is not required to have a big capacity for a huge Key algorithm computing. In other words, each node is preloaded with a set of keys from a large key pool is a distributed symmetric key management. The basic idea of the DKPS scheme is that each node randomly selects a set of keys in a way that satisfies the probability property of cover-free family (CFF). Any pair of nodes can invoke the secure shared key discovery procedure (SSD). The theory behind the SSD is the additive and scalar multiplicative homomorphism of the encryption algorithm as well as the property of non-trivial zero encryption. To discover the common secret key, one side of the two parties can form a polynomial and send the encrypted polynomial to the other side. The coefficients of the polynomial are encrypted with the sender's secret key. The other side will send back the encrypted polynomial multiplied by a random value. Because of the homomorphism and non-trivial zero encryption properties, either side can only discover the common secret key, without disclosing the other non-common keys [1].

b) Peer Intermediaries for Key Establishment (PIKE)

It is a random key pre-distribution scheme described in [7]. 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 [1].

c) Hybrid Key Management Schemes in MANETs

A robust and scalable hybrid key management for ad hoc networks is proposed in [2] and published in [3]. The nodes are grouped into clusters, and keys are distributed such that intra-cluster communication is secured using a symmetric cryptosystem and inter-cluster communication is secured using an asymmetric cryptosystem. Furthermore, threeshould cryptography is used for distributed certificate handling. The solution provides a significant improvement in the performance of the key management solution in a highly hostile environment, and scales well to large networks. However, the formation of clusters is not a trivial task.

3. ZONE-BASED KEY MANAGEMENT FOR MANETS

The zone based key management scheme is a hybrid key management schema for MANETs, based on the work of [2], [3] and the Zone Routing Protocol (ZRP)[10], where a zone is defined for each node and includes the nodes whose distance (e.g., in hops) is at most some predefined number. This distance is referred to here as the zone radius, rzone. Each node use symmetric key management inside its zone and asymmetric key management used for inter-zone security, without depending on clustering.

For simplicity and consistency, the notation descried in [2] will be used in this work, unless otherwise specified.

3.1 KEY GENERATION

The key generation within a zone is the same as the one used for intra-cluster in [2], where Node 1 generates the pair of primes (q and α) as a describer in the basic Diffie-Hellman schema, and starts calculating the intermediate values in distributed way. The first node calculates the first value α N1 and passes it to the next member with the value of the prime α. Each subsequent member receives the set of intermediary values and raises them to its own secret number generating a new set. A set generated by the ith member will have i intermediate values with i-1 exponents and a cardinal value containing all exponents. For example, node 4 receives: αN1N2N3, αN1N2, αN1N3, αN3N2 and generates: αN1N2N3N4, αN1N2N3, αN1N2N4, αN1N3N4, αN2N3N4.The cardinal value in this example is αN1N2N3N4 .

Noden raises all intermediate values to its secret value (Nn) and broadcast the set inside the zone. Each node in the zone extracts its respective intermediate value (Cn,i) to be used as local public key. Node n calculates the pair of (public, private) key, such that (Cn,n)PVn = 1 mode ø(P*Q), where P and Q are large prime generated and distributed by Node n, (Cn,n) form the public key of Node n and PVn is the prrivate key of node n. Node n distribute the pair of ø(P*Q) with (Cn,n) as it public key.

The setup time is linear since all members must contribute to generation the group key. Therefore the size of the message increases as the sequence is reaching the last members and more inter-ediate values are necessary. With that, the number of exponential operations also increases. This indicates that reducing the zone radius, will reduce the complexity of key generation. For inter-zone security, the asymmetric encryption is used in a similar way to the basic Diffie-Hellman strategy. A source node encrypts the original message with its private key as (original-message)PVsource mode (Psource* Qsource), the receiver who knows the public key of the source (Csource) and ø(Psource * Qsource) can recover the original message as (Encrypted-Message)Csource mode ø(Psource * Qsource).

The local symmetric encryption can be used between nodes inside the zone using the secret key of one node (Ni) and the local public key of the other Cn,j , sutch that if Nodei would like to encrypt a message for Nodej, Nodei uses the symmetric key = (Cn,j)1/Ni. On the other side, Nodej use (Cn,i)1/Nj, which equals to (Cn,j)1/Ni .

Because of overlapping between zones, each key is associated with the IP address (or any proper naming mechanism) of the zone leader caused its generation, each node uses its own keys for sending information and receivers determine the proper key based on the source address.

3.2 CERTIFICATE SERVICE

Threshold cryptography to be used for certificate generation, and when a node needs a certificate for its public key it issues a request for its zone members to validate its public key, nodes inside the zone who believe in the validity of the requesting node reply with partial certificate that contains the identity of the requesting node and the public key of the requesting node signed using the symmetric key of replying node. Then the requesting node collects k certificate shares and combines them to form the complete certificate, if the verification fails, the node try different combination of certificate shares. Each certificate has a life time, and has to be renewed if it expires or the cryptographic keys are renewed.

4. CONCLUSIONS AND FUTUTE WORK

The hybrid approach for key management is a promising research direction for scalable MANETs. In this paper we have proposed an enhancement on the hybrid key management approach through using the zone concept instead of using the clustering. Finding a more efficient way for creating the public key without losing the ability of creating certificates in a distributed manner is considered one way to improve the proposed schema. Future work also includes further analysis, simulation and comparison with other schemes.

REFRENCES:

[1] Aziz, B., Nourdine, E. and Mohamed, E. (2008)." A Recent Survey on Key Management Schemes in MANET". *ICTTA'08*, pp. 1-6

[2] Balasubramanian A., Misha, S. and Sridhar, R.(2004). " A Hybrid approach to key management for enhanced security in ad hoc networks". *Technical report*, University at Buffalo,NY, USA.

[3] Balasubramanian A., Misha, S. and Sridhar, R.(2005), "Analysis of a hybrid key management solution for ad hoc networks". *IEEE WCNC'05.* Vol. 4,PP. 2082- 2087.

[4] Bouassida, M., Chrisment, I. and Festor, O.(2008)." Group Key Management in MANETs". *International Journal of Network Security*, Vol.6, PP. 67-79.

[5] Capkun, S., Buttya, L., and Hubaux, P. (2003). "Self-Organized Public Key Management for Mobile Ad Hoc Networks*", IEEE Transaction on Mobile Computing*, vol.2, pp. 52-64.

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

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

[8] Chlamtac I., Conti M. and Liu, J. (2003) "Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks". Vol 1, pp.13-64

[9] Corson, S. and Macker, J.(1997). "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations". Retrieved from http://www.ietf.org/rfc/rfc2501.txt

[10] Haas Z.(1997). "A new routing protocol for the reconfigurable wireless networks". *ICUPC 97*, Vol.2, PP. 562-566

[11] Luo, H. and Lu, S. (2004). "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", *IEEE/ACM Transactions on Networking.* Vol. 12, pp. 1049-1063.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[12] Mukherjee, A., Deng, H. and Agrawal D.(2004). “Distributed Pairwise Key Generation Using Shared Polynomials for Wireless Ad Hoc Networks”. *MWCN’04*, pp. 215-226

[13] Raju, G. and Akbani, R. “Mobile Ad Hoc Networks Security” (2004). *Annual review of communications*, Vol 58, pp. 625-628

[14] Royer, E., and Toh, C. (1999). “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”. *Personal Communications*. Vol 6, pp. 46 - 55

[15] Schwingenschlogl, C. and Eichler, S.(2004). “Certificatebased Key Management for Secure Communications in Ad Hoc Networks”. *EW2004*, Retrived from http://research.ac.upc.edu/EW2004/papers/88.ps

[16] Tandler, P., Streitz, N. and Prante, T.(2002). “Roomware-Moving Toward Ubiquitous Computers”. *IEEE Micro*, Vol. 22 pp. 36-47

[17] Valle, G.and Cardenas, R.(2005). “Overview the Key Management in Ad Hoc Networks”. *ISSADS’05*, pp. 397-406.

[18] Vasiliou, A., and Economides, A. (2005). “Evaluation of Multicasting Algorithms in MANETs‖. *In Proceedings of the 3rd International Conferenceon Telecommunications and Electronic Commerce*, pp. 94-97.

[19] Wu, B., Wu, J., Fernandez, E., Ilyas, M. and Magliveras, S. (2007). “Secure and efficient key management in mobile ad hoc networks. Network and Computer Applications”. Vol. 30, pp. 937-954.

[20] Yi, S. and Kravets, R. (2004). “Composite Key Management for Ad Hoc Networks”. *MobiQuitous’04*, pp. 52-61.

[21] Yi, S., Naldurg, P. and Kravets,R (2001). “Security-aware ad hoc routing for wireless networks”. *MobiHoc’01*, pp. 299-302.

[22] Zhou, L. and Haas, Z. (1999). “Securing Ad Hoc Networks”, *IEEE Network Magazine*, Vol. 13,pp. 24-30.