A Study on the Schemes for Safeguarding Mobile Ad-hoc Networks

Neethu Mariam Joseph, Priyadharshini K
AP/IT, Karpagam College Of Engineering

***Abstract*— Security has turn out to be a primary concern in order to present protected communication between mobile nodes in an adverse environment. Mobile Ad hoc Networks are group of mobile terminals or nodes, permitting no stationary structure and centralized administration. There are a lot of vulnerable natures in the mobile ad hoc network that concerns the development of it. Unlike the wired networks the distinctive characteristics of mobile ad hoc networks create certain challenges to its security designs such as open peer-to-peer network structure, collective wireless medium, strict resource restraints, and extremely dynamic network topology. This paper first identifies from the literature the threats and challenges in mobile ad-hoc network and then discusses about the current schemes that secures the mobile ad-hoc networks.**

***Index Terms—Mobile Ad Hoc Network, Security*.**

I. INTRODUCTION

The Mobile Ad hoc Network is unprotected by its characteristics. There is not having a clear line of protection because of the freedom for the nodes to connect, leave and transferwith in the network. Certain nodes may be compromised by the opponent and thus carry out some malicious behaviors that are hard to detect. The lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator. The restricted power supply can cause some selfish problems and the continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need a strong security scheme to ensure the security of it.

A Mobile Ad hoc NETwork (MANET) is a self arranging infrastructure-less network of mobile devices associated in wireless mode. Each device in a MANET is open to move separately in any route, as a result its association changes with other devices frequently. Each device has to constantly keep the information essential to correctly route traffic is the primary confronts in building a MANET. Such networks may function by themselves or may be associated to the larger Internet. MANETs has a routable networking atmosphere, are a type of wireless ad hoc networks that works usually on top of a Link Layer ad hoc network [1]. A MANET is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Persons and vehicles can be thus internetworked in areas with no preexisting communication infrastructure or when the use of such infrastructure requires wireless expansion. In the mobile ad hoc network, nodes can straightly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other [2].

There are two types of MANETS as follows [1]: the Vehicular Ad-hoc Networks (VANETs) are used for communicate among vehicles and between vehicles and roadside equipment whereas the Internet Based Mobile Ad- hoc Networks (iMANET) are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such kind of networks usual ad-hoc routing algorithms don't apply directly.

The mobile ad hoc network has the following characteristic features:

- Unreliability of wireless links between nodes. Because of the limited energy provision for the wireless nodes and the mobility of the nodes, the wireless links connecting mobile nodes in the ad hoc network are not reliable for the communication participants.
- Constantlyvarying topology. Due to the continuous movement of nodes, the topology of the mobile ad hoc network changes continuously
- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments.

There are some main requirements that need to be achieved to ensure the security of the mobile ad hoc network. We need to be aware about those widely-used criteria to evaluate whether the mobile ad hoc network is secure or not which includes Accessibility, Reliability,Secrecy, Genuineness, Non-

repudiation, Approval, and Obscurity. Moreover, there are some other security criteria that are more specific and application-oriented which include self-stabilization , Byzantine Robustness and location privacy and which are related to the routing protocol in the mobile ad hoc network [1].

The rest of the paper is organized as follows. The notion of security in mobile ad-hoc networks are presented in Section II. The Section III presents the some schemes for securing the mobile ad-hoc networks. Finally, the paper concludes in Section IV.

II. THREATS AND CHALLENGES IN MANET

There are many attacks being there in MANETs and these attacks are challenges because the nodes can join and leave easily in the mobile infrastructure with the dynamics requests. Schematics of various attacks on individual layer are described by Al-ShakibKhanare as follows. The Application Layer may get malicious code, Repudiation attacks; Transport Layer has Session hijacking, Flooding attacks; Network Layer gets Sybil, Flooding, Black Hole, Grey Hole, Link Spoofing, Worm Hole, Link Withholding, Location disclosure etc. Data Link/MAC may possess Malicious or Selfish Behavior, Active or Passive, Internal or External attacks; Physical layer may have the Interference, Traffic Jamming, Eavesdropping attacks[1]. Mobile ad hoc networks are vulnerable to a wide range of active and passive attacks that can be introduced quite easily since all communications take place over the wireless medium. The paper [3] describes about it as follows:

A. Lack of Secure Boundaries

There is not having a clear secure *boundary* in the mobile ad hoc network, when compared with the defense available in the traditional wired network. This vulnerability originates because of its nature that gives the freedom to connect, leave and transfer inside the network.

B. Threats from Compromised nodes Inside the Network

There may have the occurrences of various link attacks between the nodes which try to perform some malicious behaviors to destruct the links.There are some other attacks that aim to gain the control over the nodes by some unrighteous means which makes the compromised nodes to execute further malicious actions. These vulnerability can be viewed as the threats that come from the compromised nodes inside the network. A good example of this kind of threats comes from the potential *Byzantine failures* encountered in the routing protocol for the mobile ad hoc network.

C. Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server. The absence of centralized management machinery makes the detection of attacks a very difficult and will obstruct the trust management for the nodes in the ad hoc network. This makes some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure.

D. Restricted Power Supply

Due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will reply on battery as their power supply method. The restricted power supply may lead to denial-of-service attacks. Moreover, a node in the mobile ad hoc network may behave in a selfish manner when it finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to cooperate with other nodes to support some functions in the network.

E. Scalability

As the nodes are mobile, the scale of the ad hoc network keeps changing all the time. It makes it hard to predict how many nodes will be in the network in the future. Thus, the protocols and facilities that are applied to the ad hoc network should be compatible to the continuously changing scale of the ad hoc network.

In the next section, a survey of several security solutions that can provide some helps to improve the security environment in the ad hoc network is presented.

III. SCHEMES FOR SECURING MANET

Security encompasses a number of attributes that have to be addressed: accessibility, reliability, validation, confidentiality, non-repudiation and authorization. The trustworthiness of mobile ad- hoc networks has additional dimensions, such as privacy, fault-tolerance, reliability, andcorrectness. [4].This portion discusses some schemes that aim in providing a secure mobile ad-hoc network.

A. Trust and Mobility-based Clustering Algorithm

Thepaper [5] proposes an approach to secure MANETs which is a solution based on an efficient *trust model and distributed algorithm* to clustering network. This method use entirely self-organized security and monitoring process to manage behaviors of nodes with low trust level. The clustering algorithm is based on the trust and mobility metric to select certification authority (CA) and to establish public key infrastructure (PKI) in each cluster. It adds a concept called *Dynamic Demilitarized Zone (DDMZ)* to protect CAs and avoid the single point of failure in each cluster. The DDMZ is formed by set

of dispensable nodes which must be confident and located at one-hop from the CA.

The trust model is based on the assumption that there are spare social relationships among nodes and every node has its own private/public key pair. Furthermore, it assumes that the initial trust nodes are honest which do not issue false certificates and each node has the capability to manage a trust table. Initially, each trust node knows the identity and public key of other trust nodes. The trust model define a trust metric (*Tm*) which takes the continuous value on the [0..1] interval. There are five roles of nodes in each cluster and each role has particular trust level which is described as follows. *CAk is a* Certification authority of cluster *k* which certificate public key of nodes belonging in the same cluster. *RAi,k is a* Registration Authority of cluster *k* assured by trust node i with $Tm(i) = 1$. The principal goal of RA is to protect CA against attackers. *GWi,j*is a gateway node ensuring a connection between two different clusters i and j. *MNi,k*represents a member node i with average trust level $Tm(i) \in [0.5 - 0.7]$ which belonging to the cluster k. Finally, *VNi,k*is a visitor node i that belongs to cluster k, it has low trust certificate, because in *CAk*and *RAj,*there are*k* nodes that need to have more information about node i behavior. The trust relationship is ensured by CAs between clusters.

Secure Distributed Clustering Algorithm (SDCA) has the following main rules:

1) Only confident nodes can be candidate to become CA.

2) Every cluster-head is CA of only one cluster and each CA has at least one confident neighbor to form DDMZ.

3) All the confident neighbors of CA, can turn out to be RA.

4) All other nodes are at a distance of maximum d-hop from the CA according the predefined size of cluster.

The algorithm chooses CA of the cluster according to tradeoff between security and stability. It is upon the sending of periodic beacons by each confident node to its neighbors at predefined interval time. Based on information existing in the received beacons and after authentication and verification of beacon's integrity, the receivers update their information and decide about their cluster position. The security parameter depends on trust metric. Two security parameters in this algorithm have been defined: the trust level and the numbers of trust neighbors of CA candidate. These parameters indicate the security hardiness of the future cluster and the degree of attacks resistance. The stability parameter is very important on clustering algorithm and is defined as cluster-head duration. The mobility metric is based on the power level. DDMZ which permit to increase security robustness of cluster and endures malicious nodes that tries to attack CA or issue false certificates.

Pros:

- Method can be simply extended to other hierarchical routing protocols.
- Single point of failure must be avoided in each cluster
- Denial-of-Service (DoS) attack over CA node is prevented
- Architecture can bemodified to any topology changes.

Cons:

- Key revocation schemes are unavailable

B. Identity Based Schemes

The paper [6] investigates about the security issues in the mobile ad hoc networks and analyze the identity based algorithm present in [7]-[10], for a secure MANET based on Intrusion Detection Systems.

1) IDDIP- An ID based Secure Dynamic IP Configuration Scheme :

An ID based Secure Dynamic IP Configuration Scheme is described in [7]. This ID based secure distributed dynamic IP (IPv4) configuration scheme, namely IDDIP is for address allocation which eliminates the need for broadcasting messages over the entire MANET during the address allocation process. This scheme provides authentication for address configuration without the help of a trusted third party while taking care of the security threats associated with dynamic IP configuration. The robustness of IDDIP scheme is medium. However, the scheme is inefficient to handle the address leak problem and also false reply attack.

2) IDSDDIP- An ID based Secure Distributed Dynamic IP Configuration Scheme:

An ID based distributed dynamic IP (IPv6) configuration scheme, namely IDSDDIP, that securely allocates IP addresses to the authorized nodes for a MANET is described in [8]. The scheme is distributed among MANET nodes. Therefore, each node has capability of generating unique IP addresses from its own IP address and can assign those addresses to the new nodes. This scheme eliminates

the need of duplicate address detection procedure thus saves the considerable network bandwidth. The scheme also eliminates the help of a trusted third party for providing validation. It also resolves the difficulties such as address leak, false reply attack of IDDIP scheme. Robustness of the IDSDDIP scheme is low as the chances of address conflictions due to network partitions and mergers are high.

3) A Novel Signature Scheme to Secure Distributed Dynamic IP Configuration Scheme:

This work, is about an ID based distributed dynamic IP (IPv6) configuration scheme to securely allocate IP addresses to the authorized hosts for a MANET without broadcasting over the entire network. The scheme is perfectly robust with low overhead and fairly low addressing latency, and is capable of holding the problems that may arise due to host failures, message losses, mobility of the hosts and network partitioning or merging. In addition this novel bilinear pairing based signature scheme authenticates and lessens the security threats associated with dynamic IP configuration. The scheme is secure against any forgery attack. Also, it does not allow *key escrow*, as the key generation and distribution is based on threshold instead of one public key generator. Since it is identity based it does not require any certificate [9].

4) Identity Based Secure AODV And TCP:

The work in [10] is about an ID based secure AODV protocol that takes care of the security issues in route discovery and maintenance phases. This work assumes two levels of security: *high* and *low*. When a path is set up both the source and the destination node verifies the authenticity of all the other nodes in the route in the high level of security. Also the authenticity of a node is also verified by its immediate downstream node. But in the case of *low* level of security when a path is set up the source and destination node verifies the authenticity of end-to-end and each intermediate node on the route verifies the authenticity of the downstream node. The scheme uses sequential aggregate signatures (SAS) based on RSA. This *ID* based secure TCP securely transmits data using the Diffie-Hellman session key for the MANET nodes. Each node have an *ID* which is evaluated from its public key for authentication purpose. A node cannot change its *ID* throughout the lifetime of the MANET. Thus, the scheme is secure counter to the attacks that are associated with AODV and TCP in MANET.

Pros:

- Provides security at bootstrap, network formation, route discovery and maintenance, and end-to-end data transmission with good QoS of MANET.

Cons:

- Focus on the attacks of *Network and Transport* layers only

C. Secure and Efficient Key Management

A secure and efficient key management framework (SEKM) [11] for mobile ad hoc networks builds PKI by applying a secret sharing scheme on an underlying multicast server group. In SEKM, the server group analyzes the certification authority (CA) and provides certificate update service for all nodes which includes the servers themselves. For efficient certificate service, a ticket scheme is introduced and an efficient server group updating scheme is used here. In SEKM framework the key is circulated to *m* shareholders. Normally, the number of shareholders is significantly less than the total number of nodes (*n*) in the network. These shareholders are named as *CA-view* or *server* nodes in short. They are basically normal nodes except holding a system private key share and are capable to produce partial certificate. It is quite straightforward to connect all servers and form a special group rather than to search each one of them separately and frequently. From a node point of view it is easy to locate the server "block" rather than each "point". From the server point of view it is easy to coordinate within the group rather than the entire network. This special group is named as multicast server group, or *server group* which consists of *server* nodes and *forwarding* nodes. The forwarding nodes within the group are regular nodes. Framework of SEKM consists of several phases namely server group formation phases; group maintenance phases; share updating phases; certificate renew/revocation phase; and handling new server nodes phase. Substructure of server group in essence creates a view of CA for certificate services and efficient share updating. The server group produces the certificate

without explicitly excluding the non-server forwarding nodes.

Pros:

- Communication efficient, bandwidth saving, and easy for management
- From a well maintained group,it is easier for a node to request service rather than from multiple "independent" service providers which may be spread in a whole area
- It is much easier for servers to coordinate within the group rather than with the entire network during the secret share updating phase

Cons:

- Lack of SEKM support to multiple server groups in large networks and in partitioned networks

IV. CONCLUSIONS

This paper has addressed some approaches for overcoming the security issues on mobile ad-hoc networks. There are still some methods which are not dealt in this paper which includes the approaches that make use of some secure protocols that are specific to certain kinds of attacks. Even though there are many approaches in the literature for mitigating the concerns in MANET, no approach is fully sophisticated to give secure mobile ad-hoc networks. Thus to deal with the concerns of security in MANETs, we need to develop a secure scheme that overcomes the worries in security which will help us to adopt MANETs more confidently.

REFERENCES

[1] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network.

[2] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Survey,".

[3] Amitabh Mishra and Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30)*, CRC Press LLC, 2003.

[4] PanagiotisPapadimitratos, Zygmunt J. Haas, "Securing Mobile Ad Hoc Networks", The handbook of ad hoc wireless networks, 2003

[5] AbderrezakRachedi ,AbderrahimBenslimane, "Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks".

[6] UttamGhosh, "Identity Based Schemes for Securing Mobile Ad Hoc Networks," 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum, pp 2514-2517

[7] U. Ghosh and R. Datta, "A secure dynamic ip configuration scheme for mobile ad hoc networks," Ad Hoc Networks, vol. 9, no. 7, pp. 1327 – 1342, 2011.

[8] U. Ghosh and R. Datta, "An id based secure distributed dynamic ip configuration scheme for mobile ad hoc networks," in Distributed Computing and Networking, vol. 7129 of LNCS, pp. 295–308, 2012.

[9] U. Ghosh and R. Datta, "A novel signature scheme to secure distributed dynamic address configuration protocol in mobile ad hoc networks," in IEEE WCNC, (Paris, France), 2012

[10] U. Ghosh and R. Datta, "Identity based secure aodv and tcp for mobile ad hoc networks," in *ACWR2011*, (India), December 18-21, 2011.

[11] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," IEEE Transactions On Dependable And Secure Computing, Vol. 3, No. 4, October-December 2006. pp. 386-399

Neethu Mariam Josephholds M.Tech in Network and Internet Engineering from Karunya University, 2013 and B.Tech in Information Technology from Anna University, 2011. The area of interests includes Cloud Computing, Computer networks and security.

She is working as Assistant Professor in the department of Information Technology, Karpagam College of Engineering. She worked as Assistant Professor in the department of Computer Science and Engineering, Karpagam University.

Ms. Neethu isa member in professional societies like IAENG and theRED.

Priyadharshini.K M.E in Computer Science and Engineering from Anna University, 2013 and B.E in Information Technology from Avinashilingam University, 2011. The area of interests includes Computer networks and security.

She is working as Assistant Professor in the department of Information Technology, Karpagam College of Engineering. She worked as Assistant Professor in the department of Computer Science and Engineering, Karpagam Institute of Technology.

Ms. Priyadharshini is a member in professional societies like IAENG and theRED.