INTRUSION AWARE GROUP MANAGEMENT SCHEME FOR MANET

P.Sumathi
Assistant Professor (SG),SNS College of Engineering, Coimbatore, Tamilnadu, India
psumathi.it@gmail.com

Abstract

MANET security has long been an issue for its infrastructure-less nature. The sort of networks gives rise to authentication and key-management problems in MANETs. The absolute TTP based schemes seem to be infeasible for being adopted in MANETs and so are the non-TTP based self-organized schemes which suffer security problems regarding key identity of nodes. A hybrid scheme can serve the purpose. One of the hybrid schemes addressed these issues effectively by pre-assigned logins on offline basis and issuing certificates being online, using 4th generation services. However, the scheme revealed overheads in different scenarios. We have proposed a scheme where the nodes having common interests, once authenticated through external resources, form a group with a single key shared for the whole group. The overlapping nodes sharing different groups facilitate authentication of other nodes communicating from those groups. In this way the external messages for authentication among the nodes of different groups can be reduced to a great extent. Denial of Service (DoS) attacks are the major problem in the MANET, because the attack consumes huge bandwidth and resources. The proposed mechanism also handles the DoS attacks.

Keywords*:* Key management, MANET, 4th generation, Denial of Service (DoS) attack

1. INTRODUCTION

The mobile Ad hoc Networks (MANETs) are infrastructure -less networks comprising mobile nodes. These nodes can move and change their location in the network. These networks are called as multi-hop networks due to limited range. All hops i.e. nodes are collectively responsible for routing and forwarding data to destination. These networks help nodes to exchange data directly without using the costly services, like Satellite, GPRS and GSM.

Intrusion detection systems (IDS) are defined by both the method used to detect attacks and the placement of the IDS on the network. An IDS may perform either misuse detection or anomaly detection and may be deployed as either a network-based system or a host-based system. This results in four general groups: misuse-host, misuse-network, anomaly-host and anomaly-network. Some IDS combine qualities from these categories and are known as hybrid systems.

1.1 Link Level Security

In wireless environment the links are susceptible to attacks where eavesdropper can easily spoof the on going communication. As there is no protection like firewalls or access control in adhoc network any node can become vulnerable to attacks coming from any direction or from any node. The results of such attacks include spoofing of the node’s identity, tampering with node’s credentials, leaking of confidential information or impersonating node.

1.2. Security Factors

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

Availability ensures the survivability of network services despite denial of service attacks [4]. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield. Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

1.3 Key Management

In general, security goals in ad hoc networks are achieved through cryptographic mechanisms such as public key encryption or digital signature. These mechanisms are supported through centralized key management where trusted Certificate Authority (CA) provides public key certificate to mobile nodes so nodes can develop mutual trust between one another. Any tampering with CA can easily compromise the security of the entire network.

The proposed mechanisms used for identification such as shared secret, public key cryptography, third party authentication provide partial solution, as they are vulnerable or unable to scale. All proposed solutions require that the mobile users make proper usage of cryptographic keys. However goal of proper management and safekeeping of small number of cryptographic keys is difficult to achieve in ad hoc network due to random mobility of nodes where continuous connectivity is not maintained.

2. PROBLEM DEFITION

Authentication is an attribute of security and failure to achieving this so far, is an obstacle for enhancing the MANET security. Here, nodes can enter or exit in a randomly manner, that leaves the MANET exposed to attacks. At small scale the authentication can be managed by the nodes themselves, as physical handshaking but at large scale it becomes complex and authentication requires the involvement of trusted third party [3]. There are schemes based thoroughly on self-organization in MANETs [6] without TTP. A hybrid form of above two approaches can also be used [10]. An ideal MANET assumes minimal third party involvement [6] before MANET formation, but such MANETs without TTP-based assumptions could be exposed to attacks. This sort of ideal MANET is still to be sought and till that time we will have to rely on TTP-based assumptions. Many schemes have been proposed so far to secure the MANET in terms of authentication, which are either insecure or require heavy computation on the side of nodes. Our research work is based on the improvement of a key management scheme termed as Tseng model [10].

The Tseng model gets the nodes authenticated in MANET by 4th generation (4G) technology [7], a future technology that supports in communicating different platforms in a transparent manner. This model allows authentication and distribution of certificates to nodes through 4G services. It assumes two kinds of nodes i.e., the General nodes called as GN and special nodes as CH. The GNs are provided with logins and passwords on offline basis and server issues certificates online, through a secure channel established by the CH, after verification of login identities. The CH is also authenticated by 4G technology like cellular network, satellite or unmanned aerial vehicles. These services are termed as WCN-AS, wide covered heterogeneous network. The cellular and satellite services provide ubiquitous availability and vast coverage area for connectivity to internet.

The Tseng model presents the authentication scenario with respect to a single CA domain, which does not accommodate the global scenario. When we see the things at global level there might be different subsidiary certificate authorities that can act as a single domain each. When the Tseng model is mapped on this global scenario it leads to substantial external message overheads of accessing server on communication among nodes from different domains.

We have optimized Tseng model in a way that helps significantly in reducing the overheads. In proposed model the nodes acquire certificates through respective servers and domains. The nodes from different domains need to verify the identities on interaction through respective servers. In proposed scheme the node once authenticated by a node in the MANET can be associated with a group of nodes having similar interests. The group is expanded up to a specific limit. An overlapping node sharing two groups facilitates authentication among both groups’ member nodes. A node once authenticated becomes a trusted node for all the nodes belonging to a group. Every group retains its keys within group and not disclosed during authentication as the overlapping node provides the self-generated symmetric keys to both nodes for establishing the communication session. In this way the overheads for Tseng model are removed by reducing verification visits outside the MANET.

Host-based IDS examine the activity on a specific host. This allows them the advantage of having greater access to the logs and files of a particular computer, while being limited in what external activity. This limits the breadth of the sensor's view, yet allows it to see greater depth and detail. In this system we use host based intrusion detection scheme in all nodes.

3. RELATED WORK

We now take a brief overview of some of the related previous papers.

In threshold cryptographic scheme, the authority of a CA is partially distributed among many t+1 network nodes, called servers, to minimize the chance of a single CA for being compromised. All the nodes' certificates are divided into n shares and distributed to these server nodes before network formation. The nodes generate their partial signatures individually and send to combiner to form a single signature and present to the asking node. This seems to be a cumbersome process to acquire a node's public key which costs more than the MANET's formation objective.

A similar scheme [4] is an improvement over the previous one on the basis of availability. Here, the CA is a fully distributed authority and any t+1 number of nodes in the MANET could behave as server nodes for the issuance and verification of public keys for the nodes. Despite the advantage of availability, the scheme looses on the side of robustness. The higher value of 't' brings availability but compromises robustness.

In KAMAN [1], there are multiple servers that are responsible for distributed authentication of all nodes in the MANET. The servers are boot-strapped with keys shared with the client nodes. The users rely heavily on servers to communicate with other users for acquiring tickets after authentication in MANET which is a bottleneck to be implemented in MANETs. Secondly, the servers are not ensured as trusted as there is no TTP involved initially.

In self-organized MANETs [6], the nodes rely on themselves for all routing, authentication and mobility management. All users issue certificates to their trustees which are verified through repositories maintained by the nodes. The scheme is self-organized but has the overheads of maintaining repositories which consumes memory and bandwidth. Secondly, the nodes blindly trust other nodes for making a new entry in the MANET.

Another scheme [9], based on pair-wise key pre-distribution by an offline authority, initializes each node with randomly selected keys out of a large key pool. The communicating nodes perform authentication by matching keys out of the key-ring. The scheme requires difficult procedure for discovering shared keys among nodes and distributing symmetric keys by offline authority.

A heterogeneous key management scheme [10] resolves the identity of nodes in MANET with the help of 4G services. In this scheme the server distributes certificates to all mobile nodes in the MANET through a special node agent using 4G services. This scheme has successfully embedded TTP with the MANET and getting the nodes authenticated. However, the scheme shows external message overheads when nodes belonging to different servers and CA domains communicate. There is a room for improvement in this scheme and can be further optimized by reducing the overheads.

Some more work in this regard has been reported in references [8], [7] and [5], but with minor relevance.

4. PROPOSED AUTHETICATION SCHEME

In Tseng model [10], the overhead tends to grow with higher proportions, as the nodes belonging to different CA domains interact with each other for every new session. We have tried to overcome these weaknesses by lowering the number of external messages coming under communication scenarios for nodes belonging to different CA. The assumptions regarding infrastructure in Tseng model are taken as pre-requisite for the proposed scheme. Our scheme is based on the following assumptions and abbreviations.

4.1. Assumptions

1) A special node (CH) is introduced as an entity having both, one homogeneous card for inter-nodes communication, and other heterogeneous card for accessing the 4G services.

2) A GN is a valid user of server on internet. Server provides nodes with logins and passwords before network formation.

3) A GN generates its public and private key pair through built-in PKI technique, the public key is signed by the server, which acts as a certificate and is exchanged with other nodes. These certificates are verified through servers for communication among nodes of different origins.

Abbreviations: SID: Server ID, NID: GN ID, GID: Group ID, PKNID: Public key of GN, EPKS: Encryption with public key of Server, A: GN, B: GN, RNID: Random number taken by GN, PWNID: GN Password, h: hash, CertS: Server Certificate issued by CA, SigS: Signature with private key of Server, T: Expiry time, OGN: Overlapping General Node, ESG1: Encryption with secret key of Group 1.

4.2 System Model

In proposed model the nodes with common interest form a group after acquiring certificates from their respective servers. The groups with unique secret keys each are formed to enhance security level as if a single secret key is shared among nodes of a single large group it boosts its chances for being compromised. Initially two nodes authenticate one another through external resources with the exchange of group ID and secret key. This ID and key is shared with each added node in the group after its verification. The group nodes authenticate one another through presenting and meeting challenges on the basis of shared secret key. In the beginning any node can act as a parent and add nodes up to a specified limit after authentication for establishing a group.

The two ways of authentication are possible in MANET, one for the nodes directly authenticated called as first neighbors, while, second being the authentication among nodes indirectly connected, called as second neighbors. The first neighbors might use secret keys established through security association while the second neighbors use group secret keys for verification and session establishment. The nodes belonging to more than a single group at one time are called as overlapping nodes which makes the communication of two nodes from different groups possible by authenticating them. The self-generated session keys are provided by overlapping nodes to the communicating nodes from different groups. These nodes authenticate one another on the basis of provided session key.

The procedure of issuing certificates to the nodes by their respective servers is defined in the following section.

4.2.1 Certificate issuance

A node having a login, that wants to become part of the MANET, sends its parameters to CH as shown in Fig. 1.

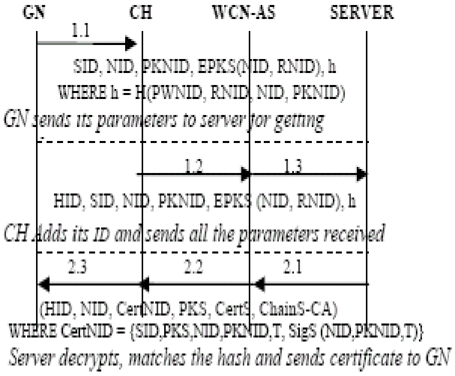

GN
CH
WCN-AS
SERVER
1.1
SID, NID, PKNID, EPKS(NID, RNID), h
WHERE h = H(PWNID, RNID, NID, PKNID)
GN sends its parameters to server for getting
1.2
1.3
HID, SID, NID, PKNID, EPKS (NID, RNID), h
CH Adds its ID and sends all the parameters received
2.3
2.2
2.1
(HID, NID, CertNID, PKS, CertS, ChainS-CA)
WHERE CertNID = {SID,PKS,NID,PKNID,T, SigS (NID,PKNID,T)}
Server decrypts, matches the hash and sends certificate to GN

Figure 1. Certificate Issuance messages along with Parameters in Tseng Model

The CH adds its ID to the message received and forwards it to the server through the secure channel. The server decrypts message with its private key and random Id (RNID) is recovered. RNID is generated on run time and put in the message by GN which is used for generating the hash. The server verifies the identity of node by comparing this hash with the received hash. On successful verification the server generates a certificate for the node by signing the node's public key. The server sends this certificate to GN along with its own certificate issued by CA within the domain. The GN receives certificate and verifies it with public key of server.

4.2.2 MANET group formation

A MANET group is formed by the nodes having common interests and objectives. Initially a node, say parent node that wants to form a group with other nodes, authenticates another node and shares a secret key by encrypting it with the public key of that node. The parent node sends the time parameter 't' along with the key. The second node checks the time period of a node's certificate while adding a node in the group. If the certificate expiry time is greater than 't', the node is authenticated and provided with the group ID and secret key, otherwise rejected. The node may be requested to renew its certificate and then become a member of that group. This group will be formed for a specific time period 't' and dispersed afterwards. The nodes in a group should be limited to a number to ensure the security level to maximum.

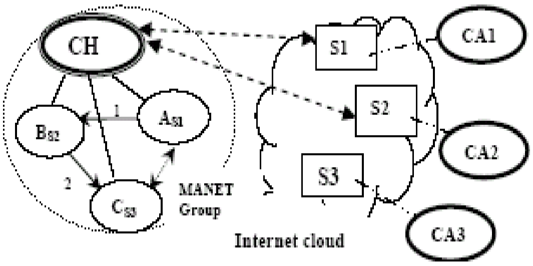


Figure 2. Authentication Scenario for the Proposed Model

In Fig. 2, the authentication scenario is shown for proposed model. The nodes A and B authenticate each other through external verification. After authentication the node A, acting as the parent node, initiates group formation with the provision of a secret key and time parameter to B. The node B in return adds a node C in the group with the same procedure. In this way a MANET group will be formed.

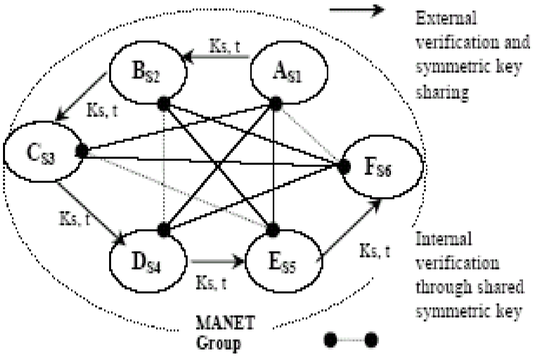

External verification and symmetric key sharing
Ks, t
B$_{S2}$
A$_{S1}$
Ks, t
C$_{S3}$
F$_{S6}$
Ks, t
D$_{S4}$
E$_{S5}$
Ks, t
Ks, t
Internal verification through shared symmetric key
MANET Group

Figure 3. MANET Group Formation and Verification

In Fig. 3, a secret key ‘KS’ is shared among all group nodes that is transferred to further nodes along with time parameter, after having them authenticated. All of the nodes can use ‘Ks’ for authenticating one another. The external messages for authentication in Tseng model are replaced with internal verification messages in proposed model.

Communication among groups by overlapping nodes If the interacting nodes belong to similar groups, the authentication is done with secret key, and for different groups it happens with the assistance of overlapping nodes. The overlapping nodes belong to more than one group and facilitate authentication of nodes from different groups by providing a self-generated temporary session key pair to the relevant nodes.

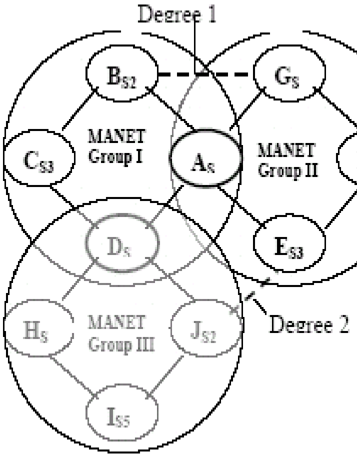


Figure 4. Communication of nodes among groups

In Fig. 4 the two overlapping nodes A and D, knowing the secret keys for both groups, assist the authentication process for rest of the nodes from both groups to communicate. Let’s call the relationship as the degree 1 linking as the nodes are directly connected with overlapping node. The communication among nodes B and G lies in degree 1 category. The communication among nodes E and J falls in degree 2 linking as the nodes are indirectly connected with the overlapping nodes; however, the two overlapping nodes lie in the same group.

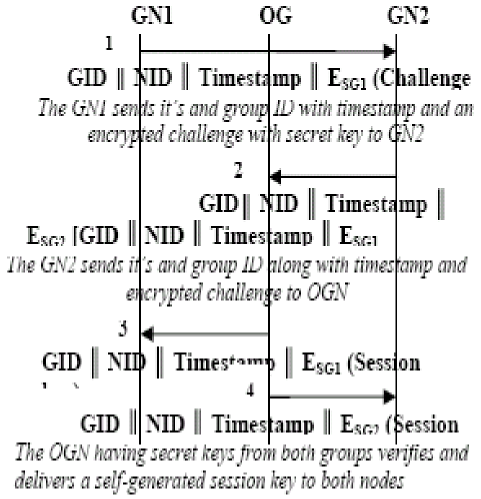
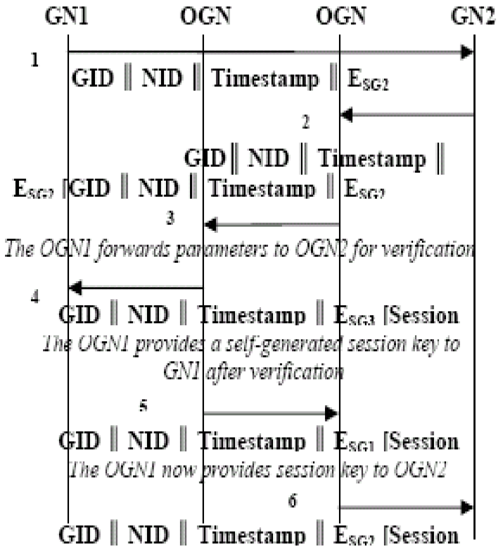

GN1
OG
GN2
1
GID ‖ NID ‖ Timestamp ‖ ESG1 (Challenge
The GN1 sends it's and group ID with timestamp and an encrypted challenge with secret key to GN2
2
GID‖ NID ‖ Timestamp ‖
ESG2 [GID ‖ NID ‖ Timestamp ‖ ESG1
The GN2 sends it's and group ID along with timestamp and encrypted challenge to OGN
3
GID ‖ NID ‖ Timestamp ‖ ESG1 (Session
4
GID ‖ NID ‖ Timestamp ‖ ESG2 (Session
The OGN having secret keys from both groups verifies and delivers a self-generated session key to both nodes

Figure 5. Authentication messages in communicating nodes of different groups facilitated by OGN of linking degree 1.

In Fig. 5, the authentication messages and parameters are shown for the communication among nodes belonging to different groups authenticated through overlapping nodes directly. In the same manner the interacting nodes might be indirectly connected with overlapping nodes.

The authentication messages for degree 2 linking are shown in Fig. 6. The scheme looses on the part of security as the linking degree for overlapping node rises.


GN1
OGN
OGN
GN2
1
GID ‖ NID ‖ Timestamp ‖ ESG2
2
GID‖ NID ‖ Timestamp ‖
ESG2 [GID ‖ NID ‖ Timestamp ‖ ESG2
3
The OGN1 forwards parameters to OGN2 for verification
4
GID ‖ NID ‖ Timestamp ‖ ESG3 [Session
The OGN1 provides a self-generated session key to GN1 after verification
5
GID ‖ NID ‖ Timestamp ‖ ESG1 [Session
The OGN1 now provides session key to OGN2
6
GID ‖ NID ‖ Timestamp ‖ ESG2 [Session

The OGN2 having secret keys from both groups verify and delivers a received session key to GN2

Figure 6. Authentication messages in communicating nodes from different groups facilitated by OGN of linking degree 2

4.2.3 MANET group dispersion

The group formed is dispersed on the achievement of a specific objective. The maximum life of a group depends upon time parameter set by the parent node. This time will be short enough to be detrimental for the MANET and can be set maximum for the objectives to be met easily. After this time the nodes cease to establish sessions with other nodes of a group. In case the objective is not met in that time, the group might be formed again with new time parameter and authentication procedures. The certificate revocation issues are irrelevant as no certificates are being issued in MANET.

4.3 Intrusion Detection Model

The intrusion detection model is designed with the signature based detection model. The signature represents the historical attack transaction flows. The signatures are maintained in signature databases such as SNORT. The signatures are compared with the current network transactions. The attacks are detected by comparing the signatures with the transactions. In the system we use the SNORT database for intrusion detection process.

5. Conclusion

In proposed model, we have tried to eliminate drawbacks in an existing key management scheme by the formation of groups in the MANET. The Tseng model reveals overheads during authentication of interacting nodes from different domains. In proposed model the nodes form several groups avail the economies of internal authentication using a symmetric shared key within each group. This key is shared among the group nodes and authentication performed internally. The overlapping nodes assist authentication process among nodes and bridging the gap among groups in MANET. This leads to cost-effective authentication using 4G services. The scheme can be regarded as an optimized extension of the Tseng and pair-wise symmetric key models. The intrusion detection model protects the nodes from attack.

REFERENCES

[1] A.Pirzada and C. Mc Donald, “Kerberos Assisted Authentication in Mobile Ad-hoc Networks”, the 27th Australasian computer science conference, 2004

[2] A.Weimerskirch, G. Thonet, “A Distributed Light-Weight Authentication Model for Ad-hoc Networks”, The 4th International Conference on Information Security and Cryptology (ICISC 2001)

[3] Azeem Irshad Sheikh, Wajahat Noshairwan, , Muhammad Rashid, Syed Mushhad Gilani, Ehtsham Irshad, Muhammad Usman “Authentication of Nodes among Different Symmetric Key Groups in MANETs using 4G Technologies ” IEEE 2009

[4] J. Kong, P. Zerfos, H. Luo and S. Lu, “Providing robust and ubiquitous security support for MANETS”. In IEEE 9th International Conference on Network Prowtocols (ICNP’01), Nov 2001; 251–260

[5] L. Eschenauer, and V. Gligor 2002. “A key-management scheme for distributed sensor networks,” Proceedings of 9th ACM (CCS’02).

[6] S. Capkun, L. Buttyan and J. P. Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks ", IEEE Transactions on Mobile Computing, Vol. 2, No. 1, Jan-Mar 2003, pp. 52-64

[7] S. Y. Hui and K. Yeung, “Challenges in the Migration to 4G Mobile Systems,” IEEE, Com. Mag. pp. 54-59, Vol. 41, 12, Dec. 2003

[8] S. Zhu, S. Xu, S. Setia, S. Jajodia, “Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach”, In 11th IEEE International Conference on Network Protocols, 2003.

[9] V. Varadharajan, R. Shankaran, M. Hitchens, “Security for cluster based MANETS” Comp. Commun. 2004; 27 (5): 488–501.

[10] Yuh-Min Tseng. “A heterogeneous-network aided public-key management scheme for mobile ad hoc networks”, Published on 10 February 2006 in Wiley InterScience, Int. J. Network Mgmt; 17: 3–15

IJAHUC-49034

http://www.inderscience.com/ospeers/admin/author/done.php?id=49034
http://www.inderscience.com
submissions@inderscience.com.
Sumathi81aathi