IJDCST @November Issue- V-1, I-7, SW-70
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Certificate Revocation Using Threshold Based Approach in Manets

[1] Kondeti.Shalini(mtech), [2] D.Swapna Mtech(p.hd)
[1] Student, PVPSIT, KANURU, VIJAYAWADA, KRISHNA DIST.
[2] Assistant Prof, PVPSIT,KANURU,VIJAYAWADA,KRISHNA DIST.

Abstract: Mobile Adhoc networks are self configurable networks. Due to this feature of the mobile Ad hoc networks security is the main aspect in present days. Certificate Revocation is an important mechanism for Manets. It plays an important role in securing Networks. Traditionally, a cluster based certificate revocation schema was used to perform quickly revoke attacker's certificate and recover their falsely accused certificates. But it has a limitation in capable of accusing malicious nodes with decreased overtime. So to identify this features we propose to develop a new method i.e. Threshold based approach to enhance cluster based certificate revocation schema. It provides quick revocation, and it immediately revokes the certificates of attackers and small overhead for control traffic. The effectiveness of the certificate schema in mobile ad hoc networks has been demonstrated through exclusive simulation results.

Keywords: Manets, certificate revocation, Certificate Authority (CA), clustering, Recovery.

I. INTRODUCTION

A mobile Ad hoc network is a self configurable infrastructure less of connecting mobile devices in wireless manner. Each mobile device can be freely rotate in dynamic way. Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes that communicate over relatively bandwidth constrained wireless links. MANETs differ from conventional wireless networks like cellular networks and IEEE 802.11 networks.

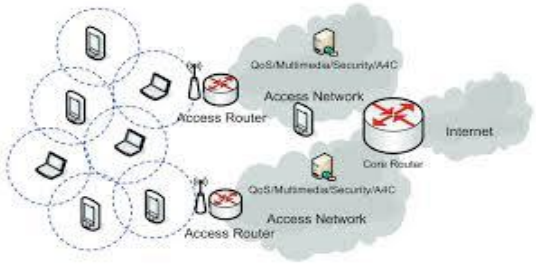

Figure 1: Mobile Ad hoc Network Architecture

MANET is a highly flexible network where nodes can freely move and join with no fixed infrastructure. Ensuring network security is one of the most important issues in MANET. MANET is an infrastructure less mobile network formed by a number of self-organized mobile nodes; it is different from traditional networks that require fixed infrastructure. In MANET nodes are free to join and leave the network at any time in addition to being independently mobile. A mobile ad hoc network is vulnerable to many kinds of malicious attacks and it is thus difficult to ensure secure communications. These unique features make MANETs very attractive for scenarios, which will require rapid network deployment. The decentralized nature of MANETs makes these network paradigms also ideal for

military and commercial applications that require high degree of robustness. Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. One of the core security issues is trust management. Trust is generally established and managed in wired and other wireless networks via centralized entities like Certificate Authority (CA). These certificates are signed by the Certificate Authority (CA) of the network. The absence of centralized entities in MANETs makes trust management security issue challenging task. The wireless technology makes MANETs more vulnerable to security attacks and due to this the traditional security methods does not provide a novel solution to MANETs.

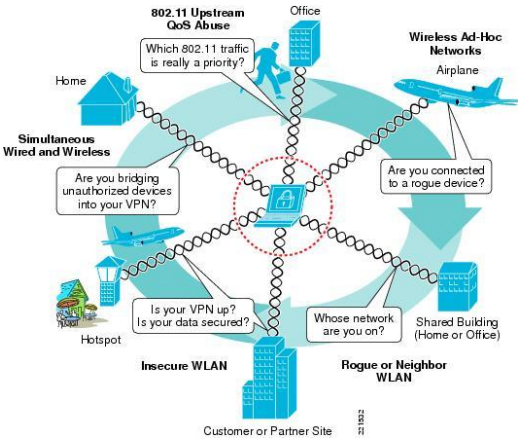

Figure 2: Manet wireless and network security integration.

Our proposed method of the security is used for detecting security considerations in real time network process. The process was developed into real time accuracy for providing security aspects presented in the transferring of data from one node to another node present in the real time network processing data.

II. RELATED WORK

URSA proposed by Luo *et al*. [2] uses certified tickets, which are locally managed in the network to evict nodes. There is no third party for the URSA. The tickets of the newly joining nodes are issued by their neighbors. The ticket of a malicious node is revoked by the vote of its neighbors because there is no centralized authority. Each node performs one-hop monitoring, and exchanges monitoring information with its neighbors that allow malicious nodes to be identified.

DICTATE [3] employs a number of CAs to efficiently perform the publication and revocation of certificates. If a CA identifies a malicious node, then the certificate of the node is revoked by the CA and its information is shared among other CAs. The certificate of a node that has been accused by just one node will be revoked by every node.

The method time session is to refresh the certificate information of each node. While this scheme is able to mitigate the damage caused by false accusations. The performance can be largely degraded by the increase of malicious nodes. CA issue CRLs that contains information about revoked certificates at regular intervals. CRLs are either placed in online repositories where they are readily available. Different certificate validation protocols are used for conventional network that are online certificate status protocol.

The certificate revocation protocol for ad hoc networks provides a measure protection against false accusation attacks. It rectifies the issue of certificate revocation without taking any input from external entities. Information that are used to decide whether the certificate of node should be revoked or not, that information is shared by all the nodes. The

responsibility is given to individual node for certificate revocation and for maintaining information about the status of the certificates of the peers with which they are communicating.

The nodes that are having valid certificate, only those nodes are allowed to enter into a network. The number of nodes 'N' using which user wants to create network that all 'N' nodes are considered as valid and thus certificate are generated for all 'N' nodes initially. The first duty of a node is to broadcast its certificate to all the 'N' nodes present in network the first duty of a node is to broadcast its certificate to all the 'N' nodes present in network after entering in to the network.

Clustering-based certificate revocation scheme that was originally proposed. Although a centralized CA manages certificates for all the nodes in the network. Cluster construction is decentralized and performed autonomously. The nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are located within the communication range of their CH. The aim of using clusters is to enable CHs to detect false accusations. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, particularly in the case where it is a CM in its cluster. Finally we will develop Threshold based mechanism for developing insurance like peak value representation of transferring data from one node consumption to another node present in real network sharing with each node attribute representation.

III. EXISTING SYSTEM

The certificate revocation protocol for ad hoc networks provides a measure protection against false accusation attacks. It resolves the issue of certificate revocation without taking any input from external entities. All trust management and key management tasks such as storage of certificate in this protocol. Validation of certificate and certificate revocation are performed on the individual nodes that are present within network except issuing of certificate.

The responsibility is given to individual node for certificate revocation and for maintaining information about the status of the certificates of the peers with which they are communicating. In this protocol the nodes that are having valid certificate only those nodes are allowed to enter into a network. The number of nodes 'N' using which user wants to create network that all 'N' nodes are considered as valid and thus certificate are generated for all 'N' nodes initially.

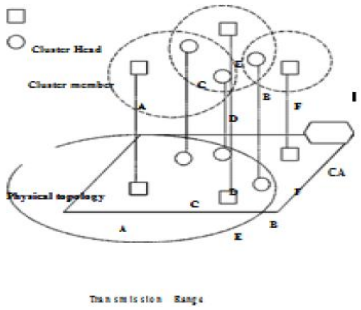

Figure 3: Node Clustering.

The information in the profile tables is used to determine whether the certificate of a given node should be revoked or not. The each node is required to compile and maintain a profile table. Designing certificate revocation scheme for MANETs that provides measure protection against false accusation attack and achieve better security. The information that is used to decide whether a certificate of node should be revoked is shared by all the nodes. To maintain the information about the certificates, the

responsibility is given to individual nodes to revoke certificates of nodes, status of the peers with which they are communicating.

IV. PROPOSED SYSTEM

To get the better and fast revocation we propose a scheme based upon a clustering-based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. To perform the clustering we use the cluster the nodes. It refers to clusters in the Manets. The scope of this scheme is to make the use of threshold cryptography and create a decentralized CA. Using threshold cryptography the duty of certificate authority is get distributed among several nodes present in the network thus the challenge related with key management service in MANETs can get resolved.

Advantages

- The proposed certificate revocation scheme for ad hoc networks, that provide some measure of protection against malicious accusation succeeding in causing the revocation of certificates of trustworthy, well-behaving nodes.
- The proposed scheme also effectively eliminates the window of opportunity whereby

  a revoked certificate can be accepted as valid.

4. SYSTEM DESIGN

4.1 Network Creation:

Build the network topology according to our requirement.Here in this modules we construct the network with the required no of nodes.

4.2 Certificate Acquisition and Certificate Storing:

In our scheme, the individual nodes within a network are responsible for all key management tasks, except issuing of certificates. Prior to entering a network, a node is required to have a valid certificate issued by a CA that is trusted by the other network peers. It is also expected to have the public keys of the CAs that issued the certificates of the peers it expects to communicate with.

4.3 Broadcasting Certificate:

The first duty of a node after entering a network is to broadcast its certificate to all the nodes.Each node in the network would have to broadcast its certificate atleast once after entering the network .This certificate would contain information such as owners id and issure id and date of issue and time of expiration.The information in the certificate would helpful to predict whether the node is trustable to communicate or not.

4.4 Request For Profile Tables:

The first duty of a node after entering a network is to broadcast its certificate to all the nodes, and simultaneously sends a request that the nodes send their profile tables. The profile table contains information about the behavior profile of each node in a network. The information in the profile tables is used to determine whether or not a given certificate should be revoked. Each node is required to compile and maintain a profile table. A profile table can be represented in the form of a packet of varied length depending on the number of accusation launched against the nodes. The length ranges from a minimum of 80 bits—when there are no accusation—to a maximum of 97(N-1)+145 bits, where _ is the number of nodes in the network. Details of the fields and content of the profile table are as follows.

1. **Owner's ID:** This field is the first 32 bits of the profile table. It contains an integer indicating the serial number of the owner's (the node that compiled the profile table) digital certificate.

2. **Node count:** this is a 16-bit field containing a short integer indicating the owner's perspective regarding the current number of nodes(N) in the network.

3. **Peer i ID:** This is a 32-bit field containing the certificate serial number of a node that is accused of misbehavior. This field also serves the purpose of a marker: if it contains zero, it indicates the end of the profile table

4. **Certificate status:** This field contains a 1-bit flag; it is set if the certificate of peer I is revoked and unset otherwise.

5. **Accusation info:** This is a 64-bit field; the first 32 bits contains an integer indicating the certificate serial number of a node that accused peer i of misbehavior. The remaining 32 bits contains the date that the accusation was made.

The information regarding the number of accusations, the identity of the accusers, the nodes being accused and the date the accusation was made, should be consistent in all the profile tables. If the node requesting the profile tables, notices any inconsistency, it is expected to launch an accusation against the node(s) that sent the inconsistent data. Profile table data is assumed to be inconsistent if it differs from the data contained in the majority of the other profile tables. Finally, the node compiles its own profile table based on the data the majority of the profile tables contain.

It should be noted that a node is allowed to accuse a given node only once throughout the lifetime of a certificate. Therefore, when an accusation is broadcast, the nodes are required to check the data in their profile tables, and add the information regarding the new accusation (certificate serial number of the accuser and the node being accused, and the date), only if there is

no prior record of the accuser accusing that particular node.

Determining the node count

Ad hoc networks are dynamic in nature: network membership and consequently the node count of a given ad hoc network, on average, changes more frequently than other networks of similar size. Our certificate revocation protocol uses the node count (N) as a parameter in certain calculations; therefore, provision needs to be made for a node to determine the number of nodes in the network at any given time.

After broadcasting its certificate, each node is required to broadcast short messages—containing its certificate serial number and the date and time that the message was sent—at a configurable time interval of T minutes. The value of T depends on the frequency of the change in the network membership. We called these messages, membership confirmation messages. When a node receives a membership confirmation message, it updates the date field associated with the certificate entry for the sender of the message, with the date indicated in the message.

If a node does not receive a membership confirmation message from any given node within 2T+1 minutes, the certificate entry for the node in question, should be deleted from the node's certificate repository. The number of entries in the certificate repository for any given node, should therefore closely reflects the actual number of nodes in the network.

4.5 Certificate Revocation:

In addition to a certificate repository, each node is required to compile and maintain a status table. Initially, it is compiled from the data in the profile table, and updated simultaneously along with the latter when a new, pertinent accusation is received. The status table is used to ascertain the status of a certificate; it consists of the following info:

Number of accusations against node i(Ai): The total number of accusations—limited to one per node—made against node i.

Number of additional accusations made by node i(Alpha i): The total number of accusations—limited to one per node—made by node I minus one.

Behavior index of node i: The behavior index of a node I (Beta i) is a number such that.0<Bi<=1. It is a measure of the status of a node amongst its peers. The greater the value of Bi, the higher the status of the given node i,Bi is computed as follows:

Weight of node i accusation (wi): The weight of a node accusation or potential accusation (if the node has not made any accusation to-date), depends on the node's behavior index and the number of accusations it made. wi is a number. such that 0<=wi<=1. It can be calculated as follows.

$$\omega_i = \beta_i - \lambda\alpha_i \quad (2)$$

Similarly, $\lambda = \frac{1}{2N-3}$, where N is the node count.

Revocation quotient (Rj) This number determines whether or not the certificate for node should be revoked. It is computed as follows:

$$R_j = \sum_{i=1}^{N} \sigma_{ij}\omega_i \quad (3)$$

$$\beta_i = 1 - \lambda A_i \quad (1)$$

$\lambda = \frac{1}{2N-3}$, where N is the node count.

If an accusation graph is constructed using the data in the profile table, such that the nodes of the graph represent the network nodes, and the edges represent accusations;

Certificate status (C i): Indicates whether or not the certificate of node i is revoked.

Underlined principle of scheme

The principal aim of the scheme we presented is to prevent malicious accusations from succeeding in causing the revocation of certificates of well-behaving, trustworthy nodes. Secondly, to eliminate or considerably reduce the window of opportunity whereby revoked certificates can be accepted as valid. Our scheme is based on the premise that all accusations should not be treated equally.

THRESHOLD BASED INTRUSION AND DETECTION SYSTEM: We present our approach of securing a MANET using threshold based intrusion detection system and a secure routing protocol was introduced. While the intrusion and detection system helps to detect attacks on data intrusion and detection processes with incorporate security features of non reputation and authentication without any availability certificate Authority mechanisms.

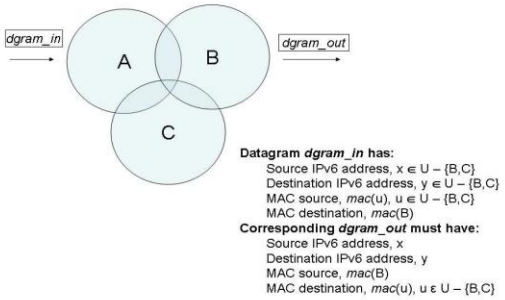

Figure 4: Monitoring traffic in ratio range with intrusion and detection system process.

As shown in the above figure we monitor data packets that need to forward. A is sending a data gram via B to some other destination, Let C be the monitoring node after B received data from A it will verify and forward other nodes present in the network data transferring process. Due to this feature of the network data processing we are sending data from sender to receiver with security considerations.

V. EXPERIMENTAL ANALYSIS

In this section we describe the experimental results for transferring data from one node religions to other node religions presented in the network efficiency. For supporting this concept procedure can be as follows:

Network Construction: It shows all the necessary components present in the network process.

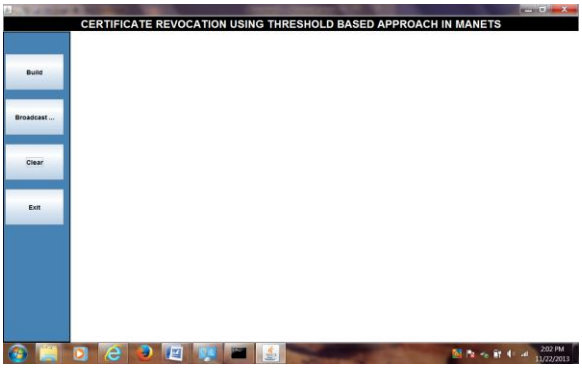

Figure 5: Network Construction

Build: Using this attribute present in the our developed network we are constructing a

Statistics	Certificate	Alpha	Beta
1	2013:Nov:22	0.2315	0.01256
2	2013:Nov:21	0.5346	0.0256
3	2013:Nov:22	0.6897	0.3256
4	2013:Nov:21	0.9874	0.0215

topology with necessary number of nodes as shown in figure 6.

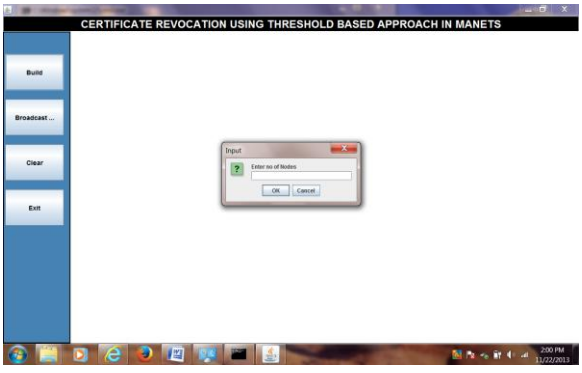

Figure 6: Build the regarding with number of nodes.

Broad Cast:

Giving an threshold value in the presented network efficiency process. In that we are giving equivalent threshold value represented in existing network process.

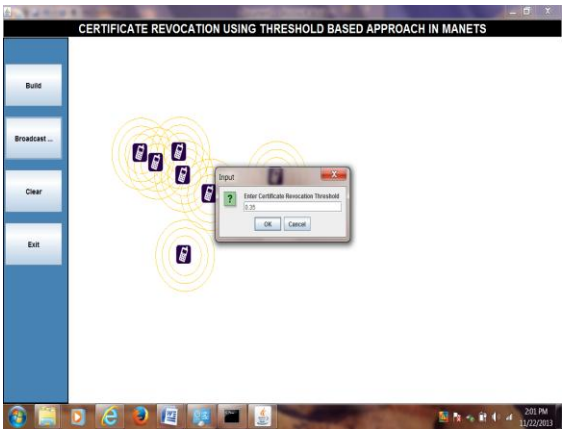

Figure 7: Network Broadcast feature in secured network.

Broadcasting features presented in the above diagram shows efficient results.

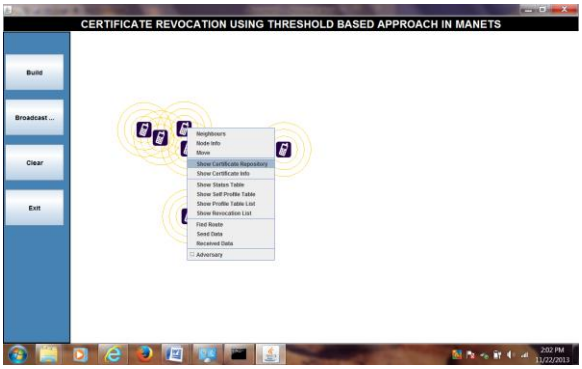

Figure 8: Performance results with direct accessing.

It will shows operations of the statics and statistics certificate results presented in networks.

Above figures shows the experimental results of the network security with certificate authority sessions presented in the network distribution process as shown in table 1

Table 1: Statistical results

VI. CONCLUSION

A cluster based certificate revocation schema was used to perform quickly revoke attacker's certificate and recover their falsely accused certificates. But it has a limitation in capable of accusing malicious nodes with decreased overtime. So to identify this features we propose to develop a new method i.e. Threshold based approach to enhance cluster based certificate revocation schema. It provides quick revocation, and it immediately revokes the certificates of attackers and small overhead for control traffic. The effectiveness of the certificate schema in mobile ad hoc networks has been demonstrated through exclusive simulation results. We present our approach of securing a MANET using threshold based intrusion detection system and a secure routing protocol was introduced. While the intrusion and detection system helps to detect attacks on data intrusion and detection processes with incorporate security features of non reputation and authentication without any availability certificate Authority mechanisms.

VII.REFERENCES

[1.] Wei Liu, Hiroki Nishiyama, N. Ansari, N.Kato, "A study on Certificate Revocation in Mobile Ad Hoc Networks", IEEE 2011.

[2] J.Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACM SIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul. 2006.

[3] Y.Joshi,T.Panke,"Study of Certificate Revocation in Mobile Ad Hoc Networks,"National Conference Entitled Fostering Management and I.T.for Gen-Next,ISBN:978-81-920972-1-3.

[4] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.

[5] G. Arboit, C. Crepeau, C. R. Davis and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Networks," Ad Ho Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[6] T.Panke,"Review of Certificate Revocation in Mobile Ad Hoc Networks,"International Journal of Advances in Management,Technology & Engineering Sciences,ISSN:2249-7455,vol.II,Issue 6(V),March 2013.

[7] Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks "School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7.

[8] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Wireless Communications, 14(5), pp. 8-20, 2007.

[9] Parker, Yesha, " Threshold Based Intrusion Detection in Ad hoc Networks and Secure AODV", Preprint submission to Ad hoc Networks, 27 Feb 2007.

[10] Jing Xie, Luis Girons Quesada and Yuming Jiang," A Threshold-based Hybrid Routing Protocol for MANET", *Department of Telematics, Norweigian University of Science and Technology*, May 2010.

[11] L. Wang and S. Olariu, "A Two-Zone Hybrid Routing Protocol for Mobile Ad Hoc Networks", *IEEE Trans. Parallel and Distributed Systems*, vol. 15, No. 12, Dec. 2004.

[12] T. Clausen and P. Jacquet, ”Optimized Link State Routing Protocol (OLSR)”, IETF RFC, MANET working group, RFC 3626, Oct. 2003.

[13] C. Perkins and E. B. Royer, ”Ad Hoc On-Demand Distance Vector (AODV) Routing”, IETF RFC, MANET working group, RFC 3561, July 2003.

[14] L. G. Quesada, ”A Routing Protocol for MANETs”, *Master thesis, Department of Telematics, Norweigian University of Science and Technology*, May 2007.