ENHANCING SECURITY IN MOBILE AD HOC NETWORKS USING CLUSTER BASED CERTIFICATE REVOCATION

Nishchitha S
PG Student,
Dept. of CSE,
BNMIT, Bangalore.

Surabhi Narayan
Associate Professor,
Dept. of CSE,
BNMIT, Bangalore.

***Abstract*— Mobile ad hoc networks (MANETs) have magnetized lot of concentration due to its mobility and ease of use. The wireless and active nature exposes them to many types of security attacks when compared to the networks. The main challenge is to provide the secure communications in the network. Certificate revocation is a method used to provide security to MANETs, which separates the attacker nodes from participating in the network activities. Here Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed to accomplish fast and precise certificate revocation process. Here all the nodes have to acquire certificates from the Certification Authority (CA). Certification Authority is responsible for certificate distribution, management and revocation among the nodes. Proposed scheme will maintain two lists Warning list and Black list, which are used to hold the accusing and accused nodes information in the network, respectively. Also this method will address the issue of false accusations in the network, where a malicious node will try to revoke the good nodes from the network by falsely accusing them as attackers. Also attacker cluster heads are identified by the Certification Authority and revoked from the network activities.**

***Index Terms*— Attacker, Certificate Revocation, False Accusation, Mobile Ad hoc Networks (MANETs), Security etc.**

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a set of mobile nodes, which are free to move across the network. Each node will consist of wireless transmitter and receiver, which is used for communicating with the other nodes in the network. Mobile ad hoc networks (MANETs) are famous due to its mobile nature, dynamic topology, and ease of deployment. It is a self-organized wireless network. It can consist of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs). Here devices will cooperate and forward data packets from one to another. By using multi hop relaying technique, nodes will extend wireless transmission range.

A. Characteristics of MANETs:

Multi hop routing: Multi hop routing technique is used by the source node, when the destination node is away from its direct transmission radius. It will use one or more intermediate nodes to forward the data to the destination.

Distributed operation: There is no central of control for the network operations in MANETs. All the network operations are distributed among all the nodes. The nodes will collaborate with each other to transmit the data. Each node can act as a relay node, to perform specific functions such as routing and security.

Autonomous terminal: Here every node is an autonomous or independent node, which can function as a host or a relay node.

Dynamic topology: Nodes are free to move in the network in any direction. Thus, the network topology will be changing frequently. The mobile devices in the MANET will perform routing among themselves as they move around.

Shared Physical Medium: The wireless communication medium is shared among all the devices in the network. Therefore access to the channel cannot be restricted.

Light-weight terminals: The devices in a MANET are with less CPU capacity, low power storage capability and less memory.

B. Applications of MANETs:

Personal area network: It is a limited coverage area and localized network. MANETs can be used to implement these Personal Area Networks. Example for short range Mobile ad hoc network is Bluetooth. Bluetooth will help in providing communication between various mobile devices like laptops, and cell phones within a limited coverage area.

Military battlefield: MANETs will help in developing and maintaining information network between soldiers, military tankers or conveyances and Head quarters. This ad hoc networking is best suited for military applications.

Emergency/Rescue operations: MANETs can be utilized in disaster mitigation operations such as in case of fire accidents, flooding or earthquake incidents. Quick deployment of communication network is necessary in the case of rescue missions. It will replace non-existing or damaged network infrastructure in the emergency fields.

Commercial applications: Commercial application of MANETs includes ubiquitous computing. Here devices will forward the data to others and data networks are formed by using the internet. An example of a practical application is the smart meters. Previously, electric meters had to be manually read by a person. Presently smart meters will report usage in real-time by using the internet.

Local Level applications: Ad hoc networks can be used to link devices like notebook computers or palmtop computers, to share the information between the members in a classroom or conference.

C. Vulnerabilities of MANETs:

Absence of centralized administration: Mobile Ad Hoc

Network will not have a centralized control unit. Because of absence of administration it is difficult to detect attacks in MANETs. It is not easy to monitor the traffic in a highly dynamic network.

Absence of predefined Boundary: In mobile ad hoc networks, it's not possible to correctly define a boundary for the network. The nodes are allowed to connect or disconnect from the network freely in MANETs. As soon as an attacker enters the transmission radius of a node, it will be able to communicate with that node.

Limited power supply: The nodes in mobile ad hoc network will have limited power, which will cause various problems. A node may behave in a bad manner when there is only limited power supply.

Cooperativeness: Nodes will cooperate and forwards the data packets from one to another. A malicious attacker can easily become a routing or relay agent and can disrupt the operations in a network.

Bandwidth-constrained links: The bandwidth of the wireless links is limited and it is expected to perform well in that limited bandwidth.

Quality of Service (QoS): Providing quality of service levels in a dynamic environment is a challenge in MANETs.

Routing: The network topology is changing constantly in the MANETs. Therefore routing of data packets between the nodes is a challenging task here.

Security is one of the major requirements for Mobile Ad hoc Networks [1, 2]. The characteristics such as dynamic or transmuting network topology and wireless nature exposes MANETs to many types of attacks. Therefore providing security is a challenging issue in MANETS. Because of open network environment, nodes will connect and disconnect freely from the network. This exposes them to various security threats. There is a need for providing secured communications and network services to the network users. Authenticity is one of the major and fundamental components of security mechanism. Certificate Management is one of the important Authentication mechanisms.

Certificate Management [3, 4] is a most widely used authentication method in the MANETs, which is used to secure network applications. Certificate is used to prove the identity of a user. It contains information about owner's identity, information about the certificate issuer and digital signature of the issuer, who is responsible for verifying the certificate contents. The signer of the certificate is called as "Certificate Authority (CA)", which will be a trusted company who will issue certificates to its customers. A Digital signature contains hash of the user details, which is then encrypted by using CA's private key. This CA's private key is not known to other users in the network. All other users in the network will be having access to CA's public key. For validating the certificates, the recipient will first calculate a fresh hash value from the sender node details. Then the recipient will decrypt the signature part in the sender node certificate using CA's public key and gets the original hash value. Then recipient will compare these two hash values generated. If both the hash values are same then only the certificate is valid. If two hash values are not similar then it clearly means that Certificate is invalid, denoting sender node details are tampered or altered by someone and hence authentication will get failed.

Certificate Revocation [6, 7, 8, 9, 10, 12, 13] is an important security component to protect the network. The wireless and dynamic network topologies make MANETs more susceptible to attackers. Certificate revocation is the process of listing and revoking the certificates of the attacker nodes and thus isolating them from further participating in the network. When an attacker node certificate is revoked, the revocation node list is broadcasted to the entire network and all the nodes in the network will updated with this information, so that attacker node is denied from all the network activities by other nodes.

Proposed Cluster based Certificate Revocation (CCRVC) scheme [11] will provide security against attacker nodes in a network. This scheme will help in quickly revoking attacker node certificate upon receiving single accusation or incrimination from any of its neighboring nodes. Also it will help in handling false accusations in the network. False accusation is a process, where a legitimate node is falsely accused as an attacker node by any of the malicious nodes in its neighborhood.

II. RELATED WORKS

Securing Mobile Ad hoc Network is a difficult task, because of the susceptibility of wireless links, the dynamic or changing network topology and the absence of network infrastructure. Certificate Revocation is a procedure used to list and cancel the certificates of the devices, which have been identified as misbehaving nodes that are launching attacks on the neighborhood. The existing Certificate Revocation procedures are classified [5] under two categories:

- Voting based schemes
- Non-voting based schemes.

A. Voting based mechanisms

In Voting based methods, attacker node certificate is revoked on the basis of total number of votes received from its neighboring nodes. It will provide high accuracy in identifying attacker node and confirming that accused node as a real misbehaving or not. Here all the neighboring nodes will exchange their voting information with each other. Certificate of an attacker node is cancelled, when total number of votes reaches the predefined threshold value. Certificate Revocation process is slow here. Voting information exchange within neighboring nodes will result in high communication overhead in the network. Also these methods will not address the issue of false accusations in the network.

Luo et al., proposed "Ubiquitous and Robust Access Control for Mobile Ad hoc Networks" (URSA) scheme [8], which is a voting-based technique to remove the attacker nodes from participating in the network. URSA technique is called as a Ticket- based approach. A Ticket consist of node ID, its public key details, ticket validity period and a signature of the ticket issuer. Without having valid tickets nodes are not allowed to access the network. The tickets for newly joining nodes are issued by its neighbors. In URSA, neighboring nodes will cooperate with each other to monitor a node's behavior and determines whether it is a legitimate or a misbehaving node, using some attack detection technique. An accusation message is exchanged locally, when a misbehaving node is identified by any of its neighbors. When the total number of accusations or votes against an accused node matches the predetermined threshold value, then that node

certificate is revoked or canceled. Here each node v_i in the network maintains two records: one is its neighboring nodes monitoring record and other one is Ticket Revocation List (TRL) record. Each record in the Ticket Revocation List consists of node ID and node's accusation list from other nodes. If node's accusation list contains k number of accusers, then that node is considered as a misbehaving node by the node v_i and marked as convicted and revocation message is flooded across the network. Determining the predetermined threshold value for the revocation is a challenge here. Another issue is URSA does not identify the falsely accused nodes in the network.

Arboit et al., proposed "A Localized Certificate Revocation Scheme for Mobile Ad hoc Networks" [9], which is a voting-based technique for attacker node certificate revocation. Here each node must acquire a valid certificate from a recognized trusted Certificate Authority (CA) and the public key of the CA. By using CA's public key, nodes in the network are able to validate the certificates of other nodes. Whenever a node detects any misbehaving nodes in the network then it will broadcast an accusation against that particular misbehaving node throughout the network. Here nodes will vote along with its weight values. The node weight is calculated based on the terms of its reliability and trustworthiness value, which is derived from its past behaviors such as total number of accusations it made against the other nodes and total number of accusations it received against itself from other nodes in the network. Here certificate of a misbehaving node is revoked when the total of accusing node weights exceeds a predetermined threshold value. In this scheme, the accuracy of certificate revocation is improved by using weight values based on trustworthiness of accusing nodes. Since all the nodes are participating in each voting, the communication overhead used to exchange voting information with each other is pretty high, and also it increases the certificate revocation time.

H. Yang et al., proposed "Self-Organized Network-Layer Security in Mobile Ad hoc Networks" (SCAN) scheme [7], which is a voting-based certificate revocation scheme used to evict attacker nodes in the network. The SCAN scheme will help in providing network-layer security for mobile ad hoc networks. It will protect both packet forwarding and routing operations in the network. Here each node will own a token in order to interact with any other nodes in the network. When a misbehaving node is detected in the network, its token revoked. Here each token is signed by the same secret key. The token can be validated by using a public key, which will be known to all the nodes in the network. In SCAN method, neighboring nodes will monitor each other for their routing and packet forwarding operations and independently detects the misbehaving nodes in its neighborhood. Attacker revocation is done by using a distributed consensus mechanism, where a node is convicted or revoked only when its multiple neighbors will detect the misbehavior and agree that particular node is malicious node. Here "m out of N" strategy is used as the consensus criteria. In "m out of N" strategy a node is determined as an attacker, if m nodes out of its N neighbors will identify its misbehavior separately. This mechanism will reduce the possibility of falsely accusing a legitimate node as an attacker node.

Dieynaba Mall et al., [12] proposed a voting based certificate revocation technique called "SECRET: A Secure and Efficient Certificate Revocation Scheme for Mobile Ad hoc Networks" to revoke attacker nodes from the network. Here every node will communicate with the Certificate Authority (CA) and acquires the certificate signed by the Authority and its public key. In this scheme, each node will maintain a Certificate Revocation List (CRL), including the details of its known nodes, their accusation details against the other nodes and accusations it received against itself from other nodes in the network. Here each node will monitor its one-hop neighboring nodes for the attacks by using Neighborhood Watch algorithm. Whenever a node finds a suspicious neighbor, it sets the accusation value from 0 (trusted) to 1 (malicious) and generates a neighborhood watch message or the accusation message. This accusation messages are protected by using a MAC function, to avoid illegal or modified accusations in the network. Then node will securely propagate this message to its one-hop neighboring nodes. Each node will update its CRL according to the received neighborhood watch message. When a node identifies that the number of accusations against any suspected node in its CRL is reaching the predefined revocation threshold value, then it will broadcast revocation message throughout the network. All other nodes in the network will update their CRL, with revoked node information. This method will results in high communication overhead in the network because of neighborhood watch message exchange between nodes. Also it increases the Revocation time required.

B. Non- Voting based mechanisms

In non-voting based methods, attacker node certificate is cancelled upon receiving single accusation from any of its neighboring nodes. Here certificate revocation process is quick. It will reduce the communication overhead, when compared to the existing voting based schemes. But accuracy of confirming a misbehaving node as a real attacker or not is degraded when compared to voting based methods. Also these methods will not able to identify false accusations in the network.

Clulow et al., [10] proposed a non-voting based revocation mechanism called "suicide for the common good" strategy to revoke attacker nodes in the network. In this scheme, attacker revocation can be quickly completed by receiving only single accusation. Here both the accused and accusing nodes are simultaneously revoked from the network. The node which detects the misbehaving node has to surrender itself, to revoke that misbehaving attacker node from the network. Whenever a node detects any attacker, it will broadcast a signed suicide note to all the other nodes in the network. This suicide note contains information about accusing node, accused node and an appended signature generated by accusing node using its private key. Upon receiving the suicide note, other nodes in the network will verify the signature by using public key of accusing node and if valid then revokes both accusing and accused nodes from the network by adding them to the blacklist. Attacker node is revoked upon receiving single suicide note or accusation. This approach reduces the time required for attacker revocation and communication overhead when compared to the voting based certificate revocation. Application of this scheme is limited

because a node has to sacrifice itself to cancel a misbehaving node in the network. This suicidal approach will not distinguish falsely accused nodes from real attacker nodes. As a result, accurateness of revocation process is degraded.

C. Motivation

Voting based methods will provide high accuracy in identifying attacker node and confirming that accused node as a real attacker node or not. Here all the neighboring nodes will exchange their voting information with each other. Certificate of an attacker node is revoked when total number of votes reaches the predefined threshold value. Certificate Revocation process is slow here. Voting information exchange within neighboring nodes will result in high communication overhead in the network. Also these methods will not address the issue of false accusations in the network.

Non-voting based methods will revoke attacker node certificate upon receiving a single accusation from any of its neighboring nodes. Here certificate revocation process is quick. It reduces the communication overhead when compared to the existing voting based schemes. But accuracy of confirming an attacker node as a real misbehaving node or not is degraded when compared to voting based methods. Also these methods will not able to identify false accusations in the network.

Proposed Cluster based Certificate Revocation (CCRVC) scheme will incorporates the merits of both existing voting based and non-voting based schemes. It will help in prompt and quick attacker node revocation. It reduces the communication overhead when compared to voting based revocation schemes. It will help in improving accuracy when compared to non-voting based schemes. Proposed CCRVC scheme will play an important role in enhancing network security in MANETs. By incorporating clustering approach, Cluster Head will detect falsely accused nodes in the network and helps in recovering back those nodes in the network. Malicious or attacker cluster heads are detected by the certificate authority. This information is broadcasted to all the nodes in the network.

III. PROPOSED SYSTEM MODEL

Proposed Cluster based Certificate Revocation (CCRVC) scheme incorporates the merits of both existing voting-based and non-voting-based attacker revocation mechanisms. It will help in accomplishing prompt revocation of attacker nodes in the network. It lowers the communication overhead, when compared to existing voting based schemes. It increases the accuracy in deciding accused node as a real misbehaving node or not, when compared to the existing non-voting based schemes. This scheme will revoke attacker nodes upon getting single allegation from any of its neighboring nodes and helps in securing the MANETs. By incorporating clustering architecture, Cluster Head will play a major role in identifying falsely accused nodes in the network and then restores these nodes back in the network. Proposed system model is depicted in Figure 1.

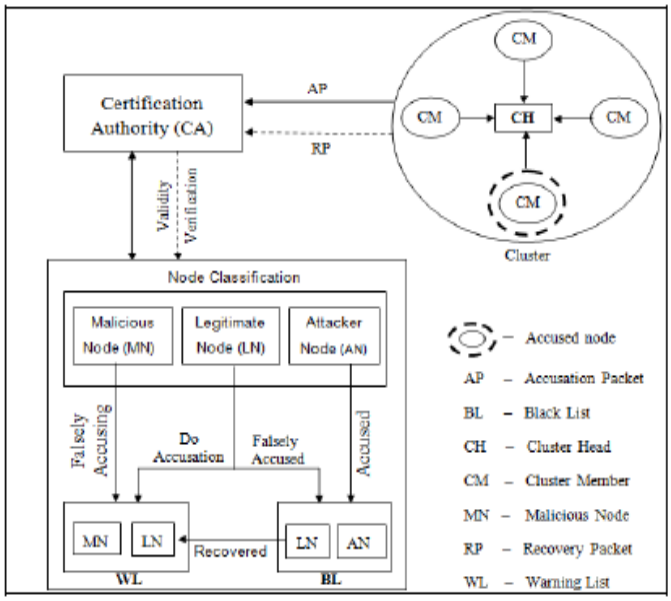

Figure 1: CCRVC System Architecture

A. Cluster Formation

Cluster Formation is the first phase in the proposed certificate revocation scheme. Here devices will cooperate with each other to form the clusters. Each cluster will contain a Cluster Head and some Cluster Members. Cluster members will be placed inside the transmission radius of their Cluster Head. Neighbor sensing protocols like periodical broadcasting of hello packets are used, to examine the existence of links between the nodes.

In this cluster construction phase initially each node will transmit a hello packet to all its neighboring nodes, along with its Energy value. The other nodes which are within transmission range of the sender node will receive this hello packet. After exchanging the hello packets, each node will compare its own energy value with other node's energy values. If the node is having highest energy value then it will become the Cluster Head. If the node is finding any one of its neighbor is having highest energy value then it will assign itself as a Cluster Member to that particular node by approving that node as a Cluster Head.

B. Certification Authority

Certification Authority (CA) is a trusted node, which is responsible for preloading the certificates to all the nodes in a network. In the certificate based authentication schemes only certified nodes are allowed to participate in the network activities. This Certificate authority is also responsible for revoking or cancelling the malicious or attacker node certificate and broadcasting this attacker node information throughout the network. Certification Authority is responsible for distributing and administering certificates of all the devices in the network.

A certificate will contain the information about its owner and the certificate authority, along with a signature

issued by the CA. Certificate Authority will generate a message digest from the original certificate content, by using SHA hash algorithm. Then encrypts this digest with its private key, using RSA Algorithm and includes this as a digital signature for the certificate. Any node in the network can check other nodes certificate integrity by using message digest function and CA's public key.

C. Node Classification

In this proposed scheme, the nodes in a network are classified into three types: Legitimate Nodes, Malicious Nodes and Attacker Nodes. A legitimate node is a well behaving node in the network. It will correctly detect the attacker nodes in its neighborhood and accuses them. It will help in revoking attacker nodes from the network and thus provides network security. A malicious node is the one which will not identify any other misbehaving nodes in the network. It will falsely accuse a well behaving node as an attacker and revokes that node from the network. An attacker node is the one which will launch the attacks and disrupts the network activities. The classification of nodes is summarized in Figure 2.

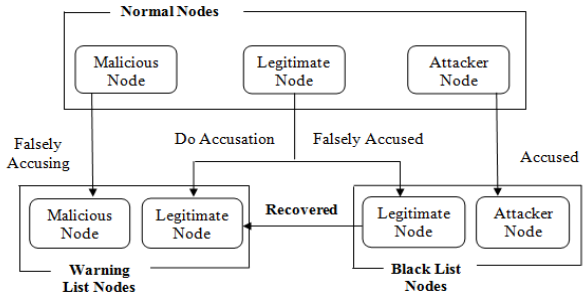

Figure 2: Classification of Nodes in CCRVC Scheme

D. Certificate Revocation

Attacker certificate revocation process contains three main stages. They are Accusation, Verification and Notification.

- ***Accusation:*** This step includes the process of detecting the attackers in the network. When a node finds an attacker in its neighborhood, it will construct an accusation packet containing attacker information and sends it to the trusted Authority, who is responsible for attacker certificate revocation.
- ***Verification:*** This step includes the process of verifying accusing node information by the trusted Authority. If accusing node is valid then authority will accept the accusation packet from that node and blacklist the accused node.
- ***Notification:*** This step includes the process of broadcasting Accusing node (Warning List) and Accused node (Black List) information to all the network nodes by the trusted authority.

The attacker revocation process starts with detecting the attacks from the attacker nodes. Then the neighboring nodes will check their local black list information whether the detected attacker node is already present in the in the list. If attacker node is not present then neighboring nodes will send accusation packet (AP) to the trusted authority (CA). The accusation packet format is shown in the following Figure 3.

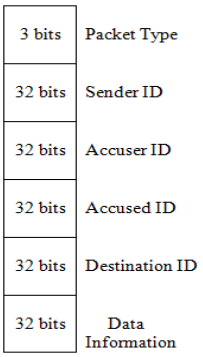

Figure 3: Format of accusation and Recovery Packets

Certificate Authority will accept the first arrived accusation packet and verifies the accusing node information. If node is valid, then the authority will conclude accused node as a genuine attacker and lists it under the Black List. Then accused node is listed under the Warning List. After updating the warning list and black list, authority will broadcast this information throughout the network. The broadcasting packet format is shown in the Figure 4.

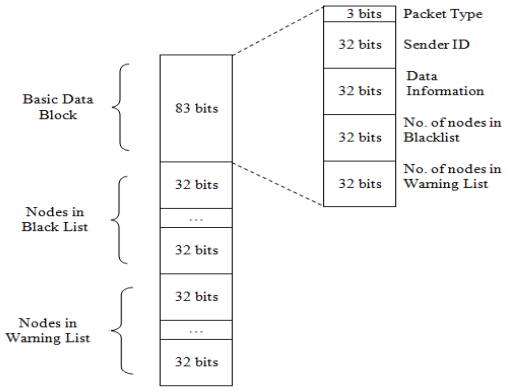

Figure 4: Format of Broadcasting Packet

E. Revoking Attacker or Malicious node Certificate

Following is the procedure for revoking the attacker or malicious node certificate.

1. Each node will monitor its neighboring nodes for detecting attacks.
2. When an attack is detected, neighboring nodes will verify

   their local Black List to check whether that attacker is already blacklisted or not.
3. If not, the neighboring nodes will send an accusation to the Certificate Authority (CA).
4. After receiving the accusation packet, the CA validates the accusing node certificate.
5. If valid, the accused node is considered as a real attacker and listed under Black List (BL). Then the Accusing node is listed under the Warning List (WL).
6. Finally, Certificate Authority will broadcast the Revocation Message, consisting of WL and BL information to all the network nodes.

7. All the network nodes will update their local Black List and Warning List information.

F. Handling False Acusations in the network

The False Accusation is a state where a malicious node is falsely accusing a well behaving legitimate node as an attacker in the network. This will result in degrading the accuracy and healthiness of the attacker revocation process. The proposed scheme will deal with these false accusations by incorporating clustered architecture. Here Cluster Head will play a major role in identifying falsely accused nodes in the network and recovering those nodes back in the network functionality. Following is the procedure for handling false accusations in the network.

1. Certificate Authority will broadcast the Warning List (WL) and Black List (BL) information to all the nodes in the network.
2. Cluster Head will check the BL, for newly added Accused Node information.
3. If any of its members are newly listed under BL, Cluster Head (CH) will run the attack detection algorithm to cross verify the blacklisted node.
4. If CH will not detect any attack from that blacklisted member, then it concludes the occurrence of the false accusation in its cluster.
5. CH sends a recovery request to the Certificate Authority, to release its member from BL.
6. Certificate Authority will accept the recovery packet from CH and verify.
7. If valid, then it will release falsely accused node from the Black List and moves it to the Warning List.
8. Certificate Authority will broadcast updated Warning List and Black List information to all the network nodes.

G. Handling Malicious or Attacker Cluster Heads

In any cluster, if Cluster Head turns into an attacker or malicious then entire network operations will get disrupted. Generally Cluster Heads will help in routing the packets from a source node to a destination, which is located outside of the transmission range of the source node. Also cluster heads are responsible for routing accusation packets from its members to the Certificate Authority. If a cluster Head becomes an attacker then all these network activities will not function properly as required. Therefore detecting attacker or malicious cluster heads in a network
is very necessary. Following is the procedure implemented to identify and handle the attacker cluster heads in the network.

1. Certificate Authority (CA) will monitor the Cluster Heads (CH) in the network for attacks, by running the attack detection algorithm.
2. If any attack is detected from any CH, then CA will black list that CH.
3. CA will broadcast this revocation message throughout the network.
4. After receiving revocation message from Authority, all the network nodes will update their local Black List information.
5. It will result in reformation of clusters and election of new cluster heads in the network.

IV. SIMULATION RESULTS

Here Network Simulator Version-2 (NS2) is used to simulate the proposed certificate revocation scheme. While we run the simulation nodes will start exchanging the hello packets and groups into clusters. Each cluster will be having highest energy node as a cluster head. After this nodes will monitor for the attacks in the neighborhood and starts sending accusation if they detect any attacker. Certificate authority will then blacklist the attacker node and sends this information throughout the network. Following Figure 5 shows the cluster formation phase, where 4 different clusters are formed in the network, Figure 6 shows attacker node (say Node 1) detection and revocation process in the network.

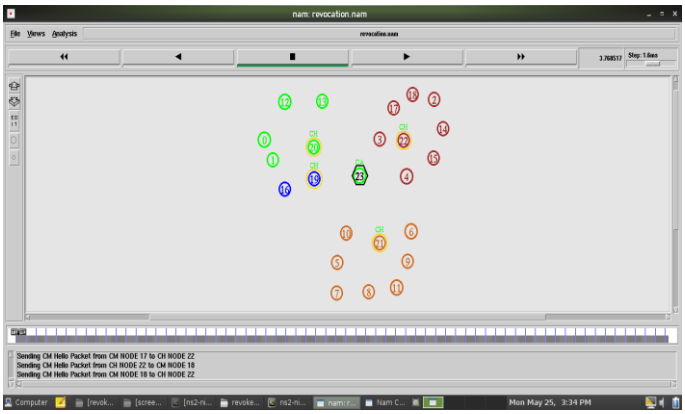

Figure 5: Cluster Formation snapshot

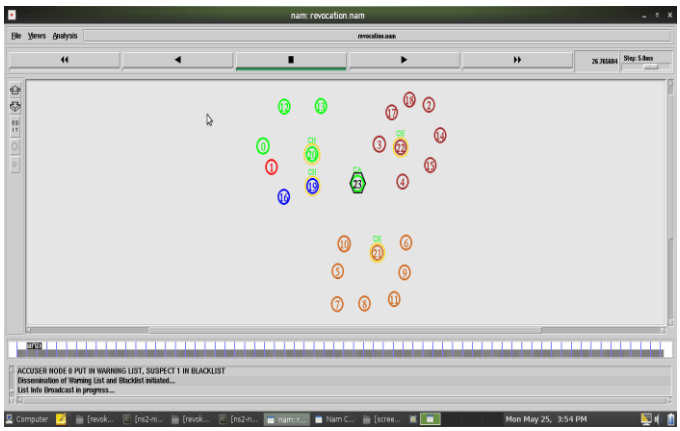

Figure 6: Attacker Node 1 Revocation snapshot

Following Figure 7 shows the xgraph, depicting the Energy Loss in the network and Figure 8 shows the xgraph, depicting the throughput in the network. In these xgraphs, both Energy loss and Throughputs with enhancement and without enhancement are compared. Enhancement part in this project is the detection and revocation of attacker or malicious cluster heads in the network.

Figure 7: Xgraph showing Energy Loss in the network

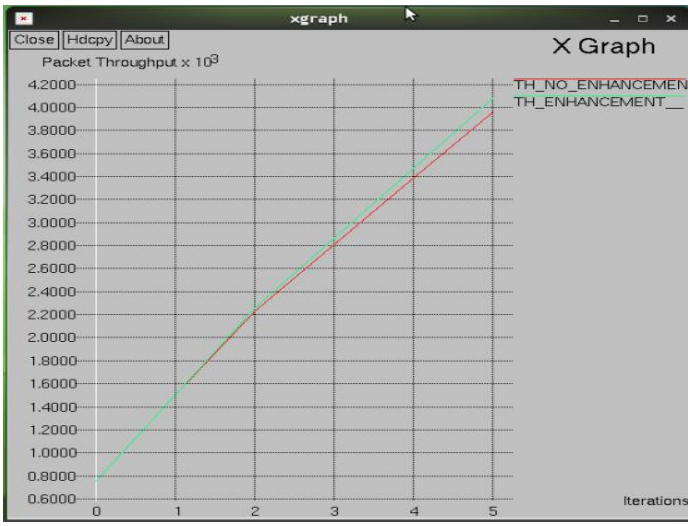

Figure 8: Xgraph showing Throughput of the network

V. CONCLUSION AND FUTURE WORKS

A major challenging issue in a Mobile adhoc network (MANET) is the secure communications between the nodes. The features such as dynamic or transmuting network topology and wireless nature exposes them to many types of attacks. Certificate Revocation technique is an important security method used to protect the MANETs. It is the procedure used for listing and revoking the certificates of the attacker nodes. When an attacker node certificate is revoked, it is denied from all the network activities by other nodes in the network. Proposed Cluster based Certificate Revocation (CCRVC) scheme will provide security against attacker nodes in the network. This scheme will help in quickly revoking attacker node certificate upon receiving single accusation or incrimination from any of its neighbors. Also this scheme will address false accusations in the network. Cluster Heads will identify falsely accused nodes in its cluster and recovers back that node in the network. Malicious or attacker cluster heads are detected and revoked by the certificate authority and this information is broadcasted to all the nodes in the network. This process will result in the reformation of clusters and election of new cluster heads in the network.

The future enhancement would be the deployment of multiple Certificate Authorities in the network. This will avoid the single point of failure in the network. If one of the CA fails in the network, then the other CA's can manage the attacker revocation process in the network. Also different CA's can monitor different areas in a network and can share the revocation details. It will be especially useful in distributed field operations, where nodes will be located over a large geographical area.

REFERENCES

[1] H. Luo, Yang, F. Ye, L. Zhang, and S. Lu, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2] N. Ansari and P. Sakarindr , "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14,no. 5, pp. 8-20, Oct. 2007.

[3] P. Spilling, A.M. Hegland, C. Rong, and E. Winjum, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[4] Z.J. Haas and L. Zhou, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[5] Mujeebudheen Khan A.I and Ann Grace Attokaren, "Survey on Certificate revocation schemes for Mobile Adhoc Networks," International journal of Computer Science and Information Technologies, vol. 5, 2014, ISSN: 0975-9646.

[6] S. Micali, "Efficient Certificate Revocation," Massachusetts Inst. Of Technology, Cambridge, MA, 1996.

[7] J. Shu, X. Meng, S. Lu, and H. Yang, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEEJ. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb. 2006.

[8] L. Zhang, H. Luo, P. Zerfos, S. Lu, and J. Kong, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6,pp. 1049-1063, Oct. 2004.

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

[10] T. Moore and J. Clulow, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems, "ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July2006.

[11] Nirwan Ansari, Jie Yang, Hiroki Nishiyama, Nei Kato, and Wei Liu, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions On Parallel and Distributed Systems, Vol. 24, No. 2, February 2013.

[12] Karim Konaté, Dieynaba Mall, and Al-Sakib Khan Pathan, "SECRET: A Secure and Efficient Certificate Revocation Scheme for Mobile Ad Hoc Networks", IEEE International Symposium on Biometrics and Security Technologies, 2014.

[13] P. T. Eugster, J. Luo, and P. Hubaux, "DICTATE: Distribute CerTification Authority with probabilisTic freshness for ad hoc networks", IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4, pp.311-323, Oct.-Dec.2005.

