Secure Cluster Head Election for Certificate Revocation in MANET

C. Annapoorani, R. Kathiroli, CSE, Anna University, MIT campus Chennai, India. cvpooran@gmail.com, kathiroli@gmail.com.

Abstract—The dynamic nature of ad hoc networks has led to the increased use of mobile nodes. Due to the absence of centralized infrastructure MANETs are prone to several threats in all layers in particular the network layer. Securing MANETs is an important factor since it plays a vital role in real time applications. In this paper a subjective trust model is proposed to elect a trusted Cluster Head is given the responsibility to revoke the certificate of malicious node there by providing secure communication. Cluster Head is elected based on the nodes stability, energy, mobility, packet delivery ratio, packet loss ratio. This algorithm aims to group the nodes into clusters for reducing the communication overhead and a trust worthy node is elected as Cluster Head in each cluster. The nodes can gain knowledge of the neighbor’s malicious activities and the nodes vote to each other based on the trust value. A voting mechanism is used by the Cluster Head to mark the node as malicious and adds it to the Certificate Revocation List. Simulations were performed to estimate trusted Cluster Head in terms of clusters, stability, overhead and throughput. The proposed method can be used to identify the Black Hole nodes in the network and provides a secure route for packet transmission in the network.

Keywords—Trust, Black Hole Attack, Certificate Revocation, Security.

I. Introduction

A Mobile ad hoc network is a system of wireless nodes dynamically self-organizing in arbitrary and temporary network topologies. Nodes in an ad hoc network can communicate without a pre-existing communication infrastructure [4]. In recent years, ad-hoc networks have been attracting increased attention from the research and engineering communities, motivated by applications like digital battlefield, asset tracking, air-borne safety, situational awareness, and border protection. Such networks are designed to operate in widely varying environments. Therefore, dynamic topologies, bandwidth constraints, energy-constrained operations, wireless vulnerabilities, and limited physical security are among the characteristics that differentiate mobile ad hoc networks from fixed multi-hop networks.

Security in Mobile ad hoc Network is the most important concern for the basic functionality of network [7]. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication.

Active Attacks: It disturbs the operation of the network and degrades the performance of the network. Some of the active attacks are malicious packet dropping attacks and routing attacks. Network layer attacks such as Black Hole, Gray Hole, Worm Hole, Sybil attack emerge during the routing process to corrupt the network. In order to make the network free from attacks security criteria must be put into service. Security mechanism [10] relies on a trusted third party to authorize the network.

To make the ad hoc networks free from attacks ad hoc network should be organized into clusters. Cluster is a method that aggregates the nodes into groups to ensure scalability and load balancing in MANET. A local coordinator called Cluster Head is elected in each cluster to manage the routing functions and the other nodes in the cluster are Cluster Members (CM). Cluster Head is elected based on the concept of trust. The trust management scheme identifies malicious activities of the node and maintains the nodes behaviour history. In this paper a subjective evaluation model beta probability distribution function is estimated to know the trust value for each node and using the trust value the nodes behaviour is estimated by the Cluster Head. The subjective trust model uses the nodes positive and negative experiences to calculate the trust value. The distributed trust computation doesn’t allow single point of failure and are precise. The routing protocol incorporated in the networks is AODV and attack considered is Black Hole Attack. The Cluster Head is assigned the responsibility to revoke the certificate of malicious node and if any false accusation is done Cluster Head takes into account to decide the node as genuine.

The rest of this paper is organized as follows. Section II discusses the related work about trust computation, leader election, certificate revocation and Section III describes about the proposed methodologies. Section IV presents the implementation. Section V portrays the conclusion.

II. RELATED WORKS

A. Trust Computation

Several trust factors are used for electing a secure Cluster Head to protect network from attacks. In Chatterjee et al., [3] employs a global weight function on each node to calculate its trust value. If the value is greater than threshold neighboring node votes for it and signs a Leader Certificate. The node that obtains many certificates is elected as Leader.

V. Palanisamy et al., [13] computes the trust value of the new node based on the recommendation certificate of the previous Cluster Head. Nomanet.al., [12] exploits a VCG mechanism to estimate the reputation of the node.
B. LEADER ELECTION
Ferdous et al., [6] presented a Cluster Head selection algorithm that includes a trust interaction table which holds the details of nodes maximum neighbors. The node which includes the maximum number of neighbor is elected as Cluster Head and others are made as Cluster Member (CM). Seunghun et al., [16] proposed a cluster based trust evaluation scheme in which neighboring nodes from a cluster and one of them is elected as a Cluster Head. The Cluster Head issues a trust certificate that can be referred to by its non-neighboring nodes but it doesn’t take the stability of the node into account.

kadari et al., [10] proposed a secured weight-based clustering algorithm and this algorithm elects Cluster Heads according to their weight computed by combining a set of parameters such as stability, battery, degree and etc.

C. VOTING MECHANISM
Luo et al., [11] uses voting based mechanism where the attackers node certificate is revoked based on the votes from valid neighboring nodes. It performs one hop monitoring and exchanges monitoring information with its neighboring nodes. If the number of nodes exceeds a predetermined number certificate will be revoked. No certification authority is used and it doesn’t handle false accusations. When the threshold value exceeds the degree of network node attacker nodes certificate can’t be revoked and collision attacks can’t be handled.

G. Arbiet et al., [1] allows all nodes in the network to vote together. Nodes vote with variable weights and weights are calculated based on reliability of nodes past behavior. Stronger the reliability greater than the weight and if the weighted sum exceeds the threshold value the nodes certificate is revoked and hence accuracy is improved. Accuracy is higher and communication is overhead is greater.

Rossanoe et al., [15] proposed a statistical inference technique belief propagation to estimate the probability of peers being malicious. The detection algorithm runs by a set of trusted monitor nodes that receives notification messages from peers whenever they obtain chunk of data; these checks contains the list of the chunk up loaders and a flag to mark the chunks polluted or clean. It defines a factor graph of peers and checks on which an incremental version of the belief propagation algorithm is run by the monitor nodes to infer the probability of each peer being a malicious one.

H. Xia et al., [21] proposed a novel trust management model that uses logic rule prediction method to evaluate the trust of nodes Fuzzy dynamic programming theory kicks out the untrustworthy nodes such that a reliable passage delivery route is obtained.

D. CERTIFICATE REVOCATION
Ms. Yogini et al., [24] proposed a Clustering based certificate revocation scheme where cluster construction is decentralized and performed autonomously. When nodes join the network, they are assumed as normal nodes. The warned nodes placed in the warning list (WL) and attacker nodes placed in the black list (BL). The certificate of the node which is in the black list is revoked by certified authority (CA), means the node is isolated from network and denied from all activities in the network. The nodes listed in the warning list can communicate to other nodes but cannot become a Cluster Head (CH) Jasaon et al., [9] proposed a light weight mechanism for revoking security certificates that is appropriate for the limited bandwidth and hardware cost constraints of a VANET. A Certificate Authority (CA) issues certificates to trusted nodes. If the CA loses trust in a vehicle (e.g., due to evidence of mal function or malicious behavior), the CA must promptly revoke the certificates of the distrusted vehicle.

Certificate organization method was used where certificates for a single vehicle are related by a single, secret revocation key. Without this key, certificates are difficult to group, there by preserving the privacy of a vehicle A revoked vehicle’s certificates can be easily identified once the revocation key is distributed via CRL. To revoke a new vehicle, the CRL need only increase in size by one revocation key and the interval for which that key was used, regardless of the number of certificates provided to the revoked vehicle requirements.

Clulowitz et al., [2] proposed a fully distributed “suicide for the common good” strategy where certificate revocation can be quickly completed by only one accusation. Certificates of both accused and accusing nodes are revoked simultaneously. It reduces the time required to evict a node and communication overhead is less. Due to suicidal approach falsely accused nodes are not taken into account and hence accuracy is degraded.

S. Diabel et al., [5] proposed a scheme to mitigate the decrease in the throughput due to the existence of a black hole in MANET, watchdogs that identify misbehaving nodes and a path-rater that helps routing protocols to avoid these nodes are used. When a node forwards a packet, the node’s watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node’s transmissions. If the next node does not forward the received packet, its failure tally is increased by the watchdog. A node is then determined as a misbehaving node by the watchdog if its failure tally goes beyond a pre-determined threshold. The path-rater then avoids such node in the future communication. Each network node runs a path-rater, which links the knowledge of a misbehaving node to its reliability before picking the most reliable route for data forwarding. Each node maintains a rating for every other known network node. The path metric is then calculated by averaging ratings of all the nodes in a given path.

I. Wouganet al., [20] proposed a modification of AODV protocol to include data routing information table (DRI) and a cross checking process. Each network node maintains its DRI table with information as to whether an intermediate node has transferred data to its neighbors and identifies misbehaviors. However, the cross checking process comes with overheads which increases end-to-end delay, as it involves the participation of every node. Furthermore, the approach may not be applicable in dynamic transmission power control routing protocols, as the transmitted data packets may not be overheard due to transmission power variations, resulting into false positive identifications.

III. PROPOSED METHODOLOGIES

A. CLUSTER CONSTRUCTION
The implementation of clustering schemes allows a better performance of the protocols for the Medium Access Control (MAC) layer by improving spatial reuse, throughput, scalability and power consumption. It also helps to improve routing at the network layer by reducing the size of the routing tables and by decreasing transmission overhead due to the update of routing tables after topological changes occur. Initially the nodes are deployed in the network and each node sends hello packet to know its neighbor. The nodes within one hop distance become the neighboring nodes. To deal with routing layer attacks and to let better routing management the nodes are to be organized into clusters. The nodes broadcast their ID to the neighbors with a REQ/REPLY flag. Cluster is constructed based on the Euclidean distance between nodes.

\[
D(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2}
\]
The distance vector allows the nodes to form clusters. The node which has maximum energy is selected as the CH and other nodes become members of the Cluster (Cluster Member). The nodes that leave from the cluster transmission range joins with other cluster by sending its ID with REQ/REPLY flag. If there is no response from any of the nodes the node forms as cluster else the node joins the cluster as one of its Cluster Member (CM)

Algorithm 1: Cluster Formation algorithm

| Input: Set of nodes  |
| Output: Set of clusters |
| Begin |
| Broadcast hello packet to find the neighboring nodes. |
| For each (node[i]) |
| Calculate \( D(p,q) = \sqrt{(p1-q1)^2 + (p2-q2)^2} \) |
| Cluster nodes with in the distance vector D for each cluster |
| if (node[i] == max(energy)) |
| Declare node as Cluster Head |
| else |
| Declare the node as Cluster Members |
| End if |
| End for |
| End |

Repeat until nodes form clusters

![Figure 1 Node Clustering](image)

**Algorithm 2: Cluster Head Election**

| Input: Set of Clusters  |
| Output: Cluster Head Election in each Cluster |
| Begin |
| Repeat for each node in cluster |
| Computes node stability |
| stability of node = \( \lambda_1 \cdot \text{NCR} + \lambda_2 \cdot \text{Energy} \) \( (\lambda_1 + \lambda_2 = 1) \) |
| Where, \( \text{NCR} = \frac{|S_i(t_1) \cap S_i(t_2)|}{S_i(t_1) \cup S_i(t_2)} \) |
| Compute the trust degree \( T(i,j) \) of node i |
| For each cluster |
| If (node[i] == max (T(i,j))) |
| Assign node[i] as Cluster Head |
| Broadcast (node[i], T(Lj)) |
| Else If (neighbour[i] == 0) |
| Declare node[i] as Cluster Member |
| For all node i in cluster j |
| Update trust table Td (i, j) |
| End if |
| End for |
| End |

B. CLUSTER HEAD ELECTION

The Cluster Head (CH) is elected based on the direct recommendation of the nodes. The direct trust value is computed based on packet delivery ratio, stability, packet drop, energy and collision factor. Each Cluster contains only one Cluster Head

Direct Trust Computation

Direct trust is established upon observations of both the successful and failure interactions of the nodes. \( \alpha \) represents the number of successful interactions and \( \beta \) represents the number of failed interactions. Positive factors such as stability, packet delivery ratio and energy are estimated as follows.

\[
\text{stability of node} = \lambda_1 \cdot \text{NCR} + \lambda_2 \cdot \text{Energy} \quad (\lambda_1 + \lambda_2 = 1)
\]

Where, \( \text{NCR} = \frac{|S_i(t_1) \cap S_i(t_2)|}{S_i(t_1) \cup S_i(t_2)} \)

\( S_i(t_1) \) and \( S_i(t_2) \) denotes the number of neighbor nodes for node i at time interval \( t_1 \) and \( t_2 \).

Energy consumed by node after time \( T \) is

\[
E = \text{packet sent} \times a + \text{packet received} \times b
\]

Where, \( a, b \) are constants. Residual Energy is analyzed based on the initial energy of the node and energy consumed.

\[
C_i = E_i - E \quad (E_i \text{ is the initial energy of the node i})
\]

The Negative parameters collision factors, packet dropped and mobility are computed using the formula (3) and (6)

Collision factor = \( \frac{\text{packet dropped}}{\text{packet sent}} \) \( (6) \)

Bayesian based Subjective Trust model

The subjective trust model is based on the beta probability density function which can be used to represent probability distribution functions. Trust degree can be represented in the form of beta PDF parameter tuple \((\alpha, \beta)\) where \( \alpha, \beta \) represents the amount of positive and negative ratings. The beta PDF denoted by \( P(\Theta/\alpha, \beta) \) can be expressed by gamma function as,

\[
P(\Theta/\alpha, \beta) = \left( \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \Gamma(\beta)} \right) \Theta^{(\alpha - 1)}(1 - \Theta)^{(\beta - 1)}
\]

Where \( \alpha = W_1 \cdot \text{Stability} + W_2 \cdot \text{Packet Sent} \)

\( \beta = W_1 \cdot \text{Packet Drop} + W_2 \cdot \text{Collision Factor} \) \( (w_1 + w_2 = 1) \)

Cluster Head election is depicted in Figure-2
C. MALICIOUS NODE DETECTION

Voting based mechanism is used for detecting malicious node. Each node votes other nodes only if the node is the most trustful one among its neighbor’s nodes and the nodes stability is better than itself. The transmission distance of vote is only one hop and the vote is not forwarded by other nodes. The better the stability it has the more trustful it is and thus with the larger probability it gets votes. The fewer the neighbors the fewer votes are obtained.

Algorithm 3 Voting Algorithm

Input: Set of Clusters
Output: Malicious Node Detection
Begin
For each node in the cluster
Each node votes for one node among other neighbors
If(max(Td(I,j)>&&sequence number>1/2 *total(CM))
    Vote++;
Else
    Vote=0;
Broadcast (vote,CH);
CH verifies the number of votes
If(votes<α)
    Declare node as malicious node
Else
    Declare as genuine node
return node to cluster
End if
End for
End;

D. CERTIFICATE REVOCATION

When the trust value of every node is calculated and a trusted CH node is elected, the CA responsibilities can be assigned to elect CH itself in the cluster. The certificate of a malicious node is revoked by the cluster Head and, it is denied from all activities and isolated from the network. For the authentication of the nodes a key id is generated for each node. To revoke a malicious attackers certificate the revocation procedure begins at detecting the presence of attacks from the attacker node.

Initially the packets are encrypted and forwarded from the source to destination. When a Black Hole attack is made by the nodes the certificate of the node is to be verified.

Certificate for the nodes are established by the providing a secret key to each cluster using SHA-1. SHA-1 algorithm is used to get hashed value from a string of plain text. The hash value will be attached to packet header for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the value attached within packet header. If they are equal, the data integrity is ensured and decrypted text is accepted; otherwise the packet is discarded. In either case, an acknowledge packet will be sent back to sender to inform of the status of the packet.
The node must provide the certificate to be in the network. If the node is unable to provide the key it is added to Certificate Revocation List. CH revokes the certificates of suspicious nodes from the network. The updated CRL is broadcasted throughout the entire network. Table -1 lists the details of certificate information table

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>1531511028573</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>NE-N-CCE</td>
</tr>
<tr>
<td>Not Before</td>
<td>DD/MM/YY</td>
</tr>
<tr>
<td>Not After</td>
<td>DD/MM/YY</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
</tr>
</tbody>
</table>

### IV. SIMULATION AND RESULTS

We used Network Simulator-2 (ns2) as simulation tool to analyze the performances of the Cluster Head (CH) election algorithm.

#### A. ENVIRONMENT

The simulation experiments are carried out in LINUX (UBANTU 10.10). In a typical simulation, our program generates a random network topology then CH election algorithms are executed by the nodes on this network topology. Simulation parameters are shown in Table-2

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>40</td>
</tr>
<tr>
<td>Traffic Pattern</td>
<td>CBR (Constant Bit Rate)</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Queue Length</td>
<td>50</td>
</tr>
<tr>
<td>Simulator</td>
<td>NS-2.34</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni directional</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Mobility</td>
<td>10.0 m/s</td>
</tr>
<tr>
<td>Pause Time</td>
<td>2.0 s</td>
</tr>
</tbody>
</table>

#### B. TRAFFIC MODEL

Continuous bit rate (CBR) traffic sources are used. The source-destination pairs are spread randomly over the network. Only 512-byte data packets are used. The number of source-destination pairs and the packet sending rate in each pair is varied to change the offered load in the network.

#### C. MOBILITY MODEL

The mobility model uses the random waypoint model in a rectangular field. Mobility models were created for the simulations using 40 nodes, with pause times of 2.0 seconds, maximum speed of 20 m/s.

#### D. RESULTS

The performance of the proposed algorithm is evaluated. Initially the actions of each node in network are normal.

**Throughput**

Packet delivery ratio (PDR) at time t is defined by

\[ \text{PDR} = \frac{\text{Packet Received}}{\text{Packet Sent}} \times 100 \]  

The packet delivery ratio changes due to varying the percentage of both cooperating and non-cooperating (malicious) nodes. Packet delivery ratio of cooperating nodes is greater than that of non-cooperating nodes. Figure 4 portrays the throughput of the nodes.

![Figure 4: Packet Delivery Ratio](image)

**Detection Rate**

It is given by number of drop packet by different number of node out of total node. If number of drop packet is more than the threshold then it is detected as malicious node. The graph shown in Figure 5 illustrates detection rate is quick so that packet loss is reduced.

![Figure 5: Packet Loss](image)

**Average End-to-End delay**

It is the average delay between the sending of packets by the source and its receipt by the receiver. The graph shown in Figure 6 represents the average delay of packets between sender and receiver.
V. CONCLUSION

Clustering decreases the communication overhead and supports for quick revocation. The trust model proposed takes into account the security requirement for the application concerned and decides the scheme of trust computation. In this paper clusters are formed based on the Euclidean distance of the nodes and Cluster Head is elected based on trust computation. A voting mechanism is used to detect the malicious node and revoke its certificate from the network and adds it to the Certificate Revocation List. Detection rate is increased whenever there is a drop in packets. Future work is to implement different types of attack exhibited by misbehavior node and detect that node to improve the performance of the network.

REFERENCES


