A NEW APPROACH TO TRUST EVALUATION FOR CLUSTER BASED MANETS

RAJKUMAR MYLSAMY, SUBRAMANIAN SANKARANARAYANAN

1Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India
2Vice chancellor, Karpagam University, Coimbatore, Tamilnadu, India
E-mail: 1rajkumar.mylsamy@gmail.com, 2drsraju49@gmail.com

ABSTRACT

A Mobile Ad hoc NETwork (MANET) is a pool of independent, dynamic, wireless devices that forms a network, devoid of no permanent infrastructure. This inherent features and wireless nature of mobile ad hoc networks makes them vulnerable to a wide variety of attacks. To discover routes with trusted nodes, we propose an approach for constructing a route without malicious nodes. To forward packets through trusted nodes, this protocol evaluates various trust parameters of neighboring nodes. To prevent a node from same attack, a weight is calculated and assigned dynamically. Simulations are done using NS2 simulator. Our proposed approach has been analyzed and evaluated for performance metrics such as packet delivery ratio, control overhead, packet drop ratio, jitter and end to end delay. Dynamic weight assignment of individual trust parameters reduces end to end delay and control overhead resulting in less packet drop ratio and high packet delivery ratio. We compare our work with other clustering algorithms, which are CBTRP and 2ACK. Our analysis and simulation result clarifies that, the proposed work effectually identifies and isolates malicious nodes and it outperforms the other algorithms.

Keywords: Mobile Ad hoc Network, Clustering, Network security, Privacy, Routing protocol

1. INTRODUCTION

A Mobile ad hoc network is a collection of mobile nodes that self-configures to form a network without any pre-established infrastructure and centralized administration [1-3]. Due to open working environment, MANETs are vulnerable to attacks by malicious nodes. Protocols used for routing in MANET can be classified as proactive [5], reactive [6, 7] or hybrid routing [8, 9]. In proactive routing method, every node consequently maintains the updated routing information. In reactive routing method, only when routing information is needed, routing information are created and maintained. Hybrid routing method is a combination of these proactive and reactive routing methods. To balance the performance and overhead of proactive and reactive routing methods, Hybrid routing scheme is proposed. As like hybrid routing methods, clustering methods [10, 11] are proposed to enhance the routing performance and to reduce complexity. A virtual partitioning of a network into a smaller sub networks, called as clustering method. Cluster Head (CH) is a node, which is having higher stability among all the members in a cluster. Also CH maintains cluster member information and topology of respective cluster information [12]. A node that connects more than one adjacent cluster is called as gateway node [13]. Since MANETs are infrastructure less and dynamic network, to protect this network from malicious nodes are hard to achieve. Existing trust value based protocols [14-16] for Cluster based MANETs, focuses on allocating trust value to a node based on considering security factors such as packet delivery ratio, packet misrouting ratio, packet alteration ratio, and packet injection ratio as collective factor, and no weight value is assigned to the separate factors that they deliberate. Based on this observation, we proposed our approach, a new trust evaluation algorithm by considering above security factors, based on the preference value assigned to each trust parameter is proposed. The objective of our approach for trust election is to deliver a predefined trust assignment for a node for cluster based MANET. The rest of the paper is deliberated as follows: Section 2 briefly explains Literature work. In section 3, the details of our routing algorithm are presented. Section 4 shows the
simulation outcomes. Finally, section 5 delivers conclusion and future work of our proposed work.

2. RELATED WORK

In this section, we present related works and background information for trust selection methods used in Mobile ad hoc networks.

Several security routing algorithms [17, 18] were proposed to address security concerns of mobile ad hoc networks. These algorithms can be classified into two groups: Cryptography-based or Reputation-based security algorithms. Cryptography based security algorithms were studied in [19, 20], and these are based on mathematical theory and computer science practice. These algorithms are either symmetric-key cryptographic algorithms, in which receiver shares the same key, or Asymmetric-key cryptographic algorithms, in which two different but mathematically related keys are used. In Reputation based security algorithms [21-23], rely on reputation and trust value of a node and are not based on cryptographic method. Several trust models have been proposed for trust management. These are centralized and de-centralized algorithms [24, 25]. In centralized algorithms (CA), trust values are maintained in centralized common node and are based on positive and negative ratings. In De-centralized algorithms (DCA), a node assigns a trust value for every visited node. The work proposes a new algorithm, based on a decentralized algorithm. Many algorithms are proposed for trust identification of a node in Cluster based routing for MANET. Trust value is evaluated in [26] based on two parameters, which is a self-evaluation of trust and sum of other nodes’ trust evaluation. In [27], Trust value of a node is analyzed based on average trust value given by neighboring nodes in a cluster. In [28], Trust is identified based on Behavior, Observation, and Belief (BOB) of a node during protocol execution. In CBTRP [29], Trust value of a node is identified based on Belief, Disbelief and Uncertainty identified by immediate neighbor nodes. If trust value is lesser than given threshold, then node is identified as malicious node, and such a malicious node is avoided in routing process. Thus, CBTRP proves better in identifying malicious nodes and packet transmission through malicious node is avoided. 2ACK scheme is proposed in [30]. In routing path, 2ACK scheme transmitting two hops acknowledgement packets in opposite direction. A, B, C are assumed as three consecutive nodes along the route. To guarantee in delivering a packet in node C, it sends 2ACK to node A. It detects misbehaving links rather than misbehaving nodes, which will cause the higher rate of packet drops.

3. PROPOSED WORK

The main objective of this paper is to provide security algorithms for cluster based MANET routing. This proposed trust model comprises three modules, Trust derivation, Trust classification and Trust computation. This model identifies malicious and non-malicious nodes in network.

3.1 Trust derivation

This module computes the trust value of a node in network. For e.g., trust value between two nodes, node ‘A’ and node ‘B’ is calculated as following. Node A takes into account individual understanding of the past transaction with another node B. The following diagram Figure 1 illustrates this.

![Figure 1: Individual understanding of neighboring nodes](image)

3.2 Trust classification

Node’s trust value is evaluated based on the following trust parameters.

1. Packet Dropping Ratio (pdr)
2. Packet Misrouting Ratio (pmr)
3. Packet Falsely injected Ratio (pfr)
4. Packet Altering Ratio (par)

Trust classification mainly based on three different values, that is High, Medium and Low values. These values are determined based on trust parameters (Packet drop ratio, Packet misrouting ratio, Packet falsely injected ratio, Packet alteration ratio).
The percentage result of each trust parameter is obtained, and these are stored in concerned linguistic variables \( d_i, m_i, f_i \) and \( a_i \). If these received values are in the range \( \{d_i<d_1, m_i=m_1, f_i<f_1, a_i<a_1\} \) { \( d_1 \leq d_2 \leq d_3 \leq d_4 \), \( m_1 \leq m_2 \leq m_3 \leq m_4 \), \( f_1 \leq f_2 \leq f_3 \leq f_4 \), \( a_1 \leq a_2 \leq a_3 \leq a_4 \} \) and { \( d_1 > d_2 > m_2 > f_2 > a_2 \) } of trust parameters pdr, pmr, pfr, and par respectively.

Then, to determine range of values High, Medium and Low values 1, 0.5 and 0 are assigned. Trust classification is handled based on the Table 1.

### 3.3 Weight assignment

Result of each trust factor is assigned in its linguistic variables \( d_i, m_i, f_i \) and \( a_i \). Node’s trust parameter value of a cluster is calculated during cluster formation process. For every node in a cluster, these values are identified for each trust parameter and then average value is calculated and stored in descending order. The maximum affected parameter is assigned with lower weight value and the least affected parameter is assigned with higher weight value. Thus, we can protect same type of attack in the network. Weight assignment calculation is represented in Table 2. From this, we can identify the weighting coefficient value for individual trust parameters.

### 3.4 Trust calculation

Trust value for a node is calculated based on variable value with concern weighting coefficient values \( \{W_{m}, W_{a}, W_{f}, W_{t}\} \). Therefore, node A’s trust on another node B is calculated as,

\[
T_{BA}^A = W_{m}(d_i) + W_{a}(m_i) + W_{f}(f_i) + W_{t}(a_i)
\]  

(1)

Where \( W_{m} + W_{a} + W_{f} + W_{t} = 1 \). If the calculated value of node’s trust is less than its relative threshold (e.g.: 0.5), then the node is assumed as malicious. Hence, it is not allowed to participate as ‘Cluster member’ in a network. Otherwise, if the calculated trust value of a node is greater than its relative threshold, then the node is assumed as non-malicious, and it is allowed to participate as a ‘Cluster member’ in a network.

### 3.5 Cluster formation

Initially, all nodes in network broadcast HELLO messages with node ID (MAC address). Nodes are updated in timed interval. Based on updated node list, each node in a network calculates its node value. Node value is computed based on the following parameters.

The degree difference \( (D_{diff}) \):

Degree difference is calculated as the difference between cluster size ‘S’ and the actual number of neighbors. It evaluates the remaining number of nodes it can handle.

\[
D_{diff} = D_{all} = d_i - S
\]  

(2)

Here, \( d_i \) is the degree of the node and is the threshold value for all nodes in the respective cluster

The Mobility of the node \( (Mob_{AB}) \):

Mobility of the node at time \( t \) is calculated using the below formula:

\[
Mob_{AB} = \frac{1}{(t_2 - t_1)} \sqrt{(p_2 - p_1)^2 + (q_2 - q_1)^2}
\]  

(3)

The remaining battery power of the node is \( E_A \).

Therefore, Stability value of Node is calculated as \( S_A = \frac{S_1 + D_{diff} + S_2 + Mob_{AB} + S_3}{E_A} \) where \( S_{1}, S_{2}, S_3 \) and \( S_4 \) are the weight values assigned and these are in a relation such that \( S_1 + S_2 = S_3 \). Depending upon the Stability value of node values, the node with the highest Stability value elects itself as CH and it is updated in Neighbor table that is present in every member of cluster. Abstract data structure for construction of a cluster is called as Neighbor table and Cluster Adjacency Table (CAT) is used for holding information about the nearby clusters. In a Cluster, CAT in CH keeps the (MAC ID) IDs of the adjacent Cluster Heads; gateway node identification (MAC ID) IDs to reach adjacent Cluster Heads. Communication of CH with an adjacent cluster is handled by Gateway node.

### 3.6 Cluster renovation

Due to the mobility in MANET, the clusters have to be restructured and reconfigured. There may be a situation where a cluster may be
reconfigured based on Stability value of cluster head (CH), node mobility, and cluster head mobility. Once TTL value of HELLO packet is 0, CH will initiate the stability factor calculation to nodes in a cluster. Each node calculates its stability value and passes it to their CH. Now CH will decide a new CH by looking at all the nodes’ stability values. This information is broadcasted to all 1-hop neighbours, and it is updated in all nodes’ NAT and CAT. When a node moves to another CH, it broadcasts HELLO message to neighbours in the cluster. The updated value of HELLO packet is verified by CH, and its stability value is analysed by CH. New node joins the new cluster and if necessary CH role is updated with new node. This information is broadcasted to all 1-hop neighbours.

3.7 Route discovery and route recovery

This section describes our algorithm, which uses trusted members, trusted heads, and trusted gateways to forward the packet from source to destination. In Route discovery, it first transmits a routing request (RREQ) message to its cluster head. The information present in RREQ message is needed for routing. The adjacent cluster head will receive the RREQ and checks RREQ message. It identifies whether it is destination. If a node is not actual destination, a Cluster head also verifies whether the given destination node addresses is present in its Neighbour table. If it is verified, then it forwards the RREQ message to one hop nearby neighbour, which is the destination. Upon delivering the ACK, source or CH or gateway saves the address of a next hop in its routing table. Till the destination CH receives RREQ, the searching of a next hop is repeated. Upon receiving RREQ message, actual destination is identified by verifying the address present in RREQ and NT. CH node forwards RREQ to destination. When the RREQ packet reaches CH, it verifies the next node is a trusted one or not, by verifying a trust factor less than 0.5. After assuring the next node is malicious, immediately it identifies another path to destination. Hence, the malicious node is isolated and it is protected from the routing process. Route recovery will be initiated if any route failure occurs. If a route failure is identified due to nodes’ mobility in the intermediate clusters, the defined path should be reconstructed and restarted either from the local node of cluster where route failure is discovered or from the source CH.

4. SIMULATION RESULTS

4.1 Simulation parameters

Our proposed work is performed using the NS2 network simulator. IEEE 802.11 standard is used as MAC layer protocol. The radio propagation model used is the Two-Ray ground model. Nominal transmission range is 250 meters. The radio model is simulated with a nominal bit rate of 11 Mbps. The traffic type is Constant Bit Rate (CBR) with network packet rate of 4 packets/sec, and the packet size is 512 bytes. The movement model used is a Random way point model. The pause time used is 0 second. The simulation time used is 800 second. The value of High, Medium, and Low for Trust classification are 1, 0.5 and 0 respectively. The value of Weights for identifying stability factors and are 0.5 and 0.5 respectively. The value of d factors for packet delivery ratio d1 and d2 are 5% and 10%.

4.2 Packet delivery ratio

The ratio of total number of packets brought to the destination node to the total number of packets sent from the source node is defined as Packet delivery ratio. Figure 2, It shows that during transmission, intermediate nodes have several routes to the destination node so that when detecting malicious nodes, they can try an alternate route to forward packets and thus improve the packet delivery ratio. This shows that the proposed our approach can efficiently deliver the packets by detecting and isolating misbehavior nodes than CBTRP and 2ACK.

![Packet delivery ratio of our approach, CBTRP and 2ACK](image_url)

4.2.1 Control overhead

Our proposed approach is simulated using different factors. Figure 3, shows that our proposed approach is more efficient as compared to CBTRP and 2ACK.
The ratio of the number of control packets (route request, route reply, error packets, sequencing) transmitted to the number of data packets delivered is defined as Control overhead. Figure 3 shows that our approach is very efficient in terms of control overhead in data delivery. The work analyses the control overhead in our approach, CBTRP and 2ACK on two conditions (with and without considering malicious nodes).

Control overhead of our approach is less than CBTRP and 2ACK. Our proposed approach does not do cluster head re-election process periodically for cluster maintenance.

4.3 Throughput

The percentage of misbehaving nodes versus average aggregated throughput is shown in Figure 4.

As a comparison, CBTRP and LEACH methods are simulated to find the relationship between percentage of misbehaving nodes and throughput. Misbehaving nodes are increased from 20% to 80% of total nodes, and the results show that the proposed method outperforms CBTRP and LEACH in terms of throughput.

4.4 Jitter

It is a measure of variability over time of packet latency across a network. A network has a jitter only if it has a variation in latency.

Jitter also called as Packet delay variation can result in both increased latency and packet loss. As Figure 5 shows, the jitter value is very low in comparison with CBTRP and LEACH. This is because of unprocessed traffic in a node. Since the proposed work considers individual trust parameters for isolating misbehaving nodes, it protects same node is affected. It is significantly less compared to others.

4.5 Packet dropping

Figure 6 shows the result of packets drop for the schemes when the number of misbehavior node is increased. From the result, we can see that our proposed work has significantly less packet drops than the CBTRP and 2ACK. This is because of our approach is immediately isolating the misbehavior nodes from trusted nodes.
5. CONCLUSION

The existence of malicious nodes in routing process for cluster based MANET have motivated us to propose an integrated solution for preventing malicious nodes in routing. Every member of cluster in a network monitors the behavior of each other in a cluster and updates their trust values. Our work proposes a well-defined trust election by considering various security parameters. The proposed work has the capability of preventing packet dropping packet injection, packet altering and packet misrouting attacks. Our work is compared with CBTRP and 2ACK. The simulation results illustrates that the proposed model can able to prolong the lifetime and forms stable clusters with most suitable one as cluster head and forwarder. This can be concluded that, our proposed approach would form the foundation for trust enabled and stable communication in MANET. The proposed work can be extended to design trustworthy forward paths to avoid link failures in a cluster based MANET routing.

REFERENCES:


### Table 2: Weight Assignment To Trust Factors

<table>
<thead>
<tr>
<th>Trust parameters</th>
<th>Node $n_1$</th>
<th>Node $n_2$</th>
<th>---</th>
<th>Node $n_m$</th>
<th>Average value (Avg)</th>
<th>Before sorting</th>
<th>After sorting (Descending order)</th>
<th>Weight assignment ($W_{duo/ua}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdr</td>
<td>$n_1(d)$</td>
<td>$n_2(d)$</td>
<td>---</td>
<td>$n_m(d)$</td>
<td>$pdr = \sum_{i=1}^{n} \frac{d_i}{n}$</td>
<td>Pdr</td>
<td>pmr ($W_m$)</td>
<td>$W_1$</td>
</tr>
<tr>
<td>pmr</td>
<td>$n_1(m)$</td>
<td>$n_2(m)$</td>
<td>---</td>
<td>$n_m(m)$</td>
<td>$pmr = \sum_{i=1}^{n} \frac{m_i}{n}$</td>
<td>Pmr</td>
<td>par ($W_a$)</td>
<td>$W_2$</td>
</tr>
<tr>
<td>pfr</td>
<td>$n_1(f)$</td>
<td>$n_2(f)$</td>
<td>---</td>
<td>$n_m(f)$</td>
<td>$pfr = \sum_{i=1}^{n} \frac{f_i}{n}$</td>
<td>Pfr</td>
<td>pdr ($W_d$)</td>
<td>$W_3$</td>
</tr>
<tr>
<td>par</td>
<td>$n_1(a)$</td>
<td>$n_2(d)$</td>
<td>---</td>
<td>$n_m(a)$</td>
<td>$par = \sum_{i=1}^{n} \frac{a_i}{n}$</td>
<td>Par</td>
<td>pfr ($W_f$)</td>
<td>$W_4$</td>
</tr>
</tbody>
</table>