NEIGHBOR NODE DISCOVERY AND TRUST PREDICTION IN MANETs

Ms. Suganya Devi.S,
PG scholar, Department of CSE,
Adhiyamaan college of Engineering,
Hosur, Tamilnadu, India.

Dr.D.Thilagavathy,
Professor, Department of CSE,
Adhiyamaan college of Engineering,
Hosur, Tamilnadu,India

ABSTRACT

MANETs are self configuring autonomous networks that do not require any central authority to control and coordinate the network. Neighborhood discovery (ND) is the process of discovering the devices that are directly reachable for communication or in physical proximity. It becomes a fundamental requirement and building block for various other applications. It is easy to abuse ND and thereby compromise the overlying protocols and applications. Thus, providing methods to mitigate this vulnerability and secure ND is crucial. This paper uses the directional antenna algorithm called as scanning based direct discovery algorithm to discover the neighbors. To enable cooperative working of the various distributed protocols we use trust system to provide the trust level of various nodes, thereby enhancing the cooperation among the nodes. This paper uses distributed hybrid trust algorithm and also uses relationship maturity concept to compute the trust of the nodes. This paper demonstrates that Trust systems are better than already existing cryptographic techniques.

Keywords: - Ad hoc networks, Neighbor discovery, Relationship maturity, Trust

I. INTRODUCTION

The most important requirement of the ad-hoc networks is that they are “self-configuring” i.e., that a large number of wireless nodes organize themselves to efficiently perform the tasks required by the application after they have been deployed.

After nodes are deployed, they do not have knowledge about the neighbors thus, they need to discover their neighbors in order to communicate with them. Knowledge of the neighbors is essential for almost all routing protocols, medium-access control protocols and several other topology-control algorithms. Neighbor discovery is, therefore, a crucial first step in the process of self-organization of a wireless ad-hoc network.

The neighbors can be either physical neighbors or communication neighbor [8]. The physical neighbors are those that are in the range of physical proximity of the discoverer. The communication neighbors are those that are reachable for communication but need not to be in the physical range of the discoverer.

The types of neighbor discovery algorithms are direct discovery algorithm or gossip based algorithm. The various other parameters used to classify the discovery algorithms are known or unknown number of neighbors, synchronous or asynchronous nodes in network. [1] We use direct discovery algorithm to discover the physical neighbors.

Since almost all the protocols deployed in the Ad hoc networks are distributed, cooperation among the nodes is very essential. To ensure the cooperation among nodes, the network should not contain any malicious nodes. We use trust management system to predict the trust level of the node. Trust metric is useful not only to identify the malicious node but also when the nodes exchange information with each other.

In this paper we use distributed trust (i.e.) every node will calculate the trust level of every other node. The centralized trust systems require a centralized trust agent to calculate the trust level of every node in the system. But this system may be compromised completely if the trust agent is compromised.

The proposed system uses both direct trust computation as well as receive recommendations from the neighbors. The concept of relationship maturity [6] is used in the proposed model to provide weights for the recommendations received from the neighbors. The recommendations from neighbors who are known for longer period of time will be given more weight than those from the newer neighbors. This could reduce the probability of false recommendations.

The proposed system uses neural network which has the ability to learn by itself, to implement the trust systems. The neural networks have the ability to build more flexible and dynamic trust systems that can be retrained to thwart a multitude of attack patterns easily and efficiently.

The paper is divided into following sections as Section II describes the existing Neighbor Discovery algorithms; Section III describes the Trust Computation Techniques; Section IV explains the Proposed Model; Section V describes the Experimental Setup.

II. NEIGHBOR DISCOVERY ALGORITHMS

The neighbor discovery algorithms can be classified as Deterministic or Random, Directional or Omni - directional Antenna based, Location based approaches, and direct discovery or Gossip based algorithms.
In randomized neighbor discovery [1], each node transmits at randomly chosen times and discovers all its neighbors by a given time with high probability.

In deterministic neighbor discovery [1], on the other hand, each node transmits according to a predetermined transmission schedule that allows it to discover all its neighbors by a given time with probability one.

The antenna models used in ad hoc networks are Omni directional antenna model or directional antenna model.

The Omni directional antenna model [10] propagates signal in all directions. The algorithm used by Omni directional antenna is 1-way algorithm where the receiver will not send any acknowledgement after receiving the discovery message. The sender broadcasts the DISCOVER message to advertise itself. The receivers will discover one neighbor if it receive the DISCOVER message correctly in the listen state.

The Omni directional antennas have drawbacks like reduced gain, increased signal distraction, high bandwidth consumption, and increased noise.

Directional antennas provide longer transmission range and higher data rate. They strongly reduce signal interferences in unnecessary directions and reduce jamming susceptibility.

The directional antenna algorithms used to discover neighbors. The radiation pattern of directional antenna is shown in figure 1.

![Figure 1 Radiation pattern of directional antenna](image)

In direct discovery algorithm [9] the nodes discover the neighbors which communicate with it directly. The method used to discover the neighbors is recording the angle of arrival of the beacon signal, determining the location based using GPS. The direct discovery algorithm will discover only those neighbors that communicate with it directly.

In gossip based algorithm [9] the neighbors are discovered indirectly through the interaction with other neighbors. Messages are exchanged to discover the neighbors. The message consists of the list of neighbors’ IDs and their locations. The main drawbacks of gossip based algorithm are message length grows as more and more nodes are discovered and the presence of physical obstacles can cause nodes to incorrectly infer another node as its neighbor.

The Direct Symmetry Test and Cross Symmetry Test was proposed in [5] is used to verify the position of the neighbors that the nodes declare.

III. TRUST MODEL

Trust is an important aspect of mobile ad hoc networks (MANETs). It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust is very important in the distributed collaborative environment. Collaborations and information sharing are considered to be essential operations in the MANET to achieve the deployment goals such as sensing and event monitoring. Collaboration will be productive only if all participants operate in a trustworthy manner.

MANETs are usually deployed in harsh or uncontrolled environments, thereby heightening the probability of compromises and malfunctioning as there is no centralized control unit to monitor the node operations. These characteristics force a component node to be cautious when collaborating / communicating with other nodes as the behavior of nodes change with time and environmental conditions. Therefore, establishing and quantifying behavior of nodes in the form of trust is essential for ensuring proper operation of MANET.

Trust computations consist of three components: ‘experience’, ‘recommendation’ and ‘knowledge’. The ‘experience’ component of trust for each node is directly measured by their immediate neighbors and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as ‘recommendation’ part of the trust. At a regular interval, the previously evaluated trust is included in the current ‘knowledge’ component of total trust.

The work on trust computations can be broadly classified into the following categories [4]:

- **Distributed trust computations**: Every node computes its own value of trust on its neighbors
- **Centralized trust computations**: central agent manages/helps the node in trust computations
- **Hybrid trust computation**: In Hybrid trust on a node is computed based on direct experience and also recommendations from other nodes

The Bayesian Approach used in [3], varies the weights for information according to their occurrence time and providers. It uses exponential decrease method to expire the old observations.

The trust model proposed in [2] contains two modules namely, Monitoring Module (MM) and Reputation Handling Module (RM). The MM monitors the packet forwarding activities of the node and the RM is responsible for managing the reputation information.

IV. PROPOSED SYSTEM

A. SYSTEM MODEL

The initial step in the setting up the Ad Hoc networks is the neighbor discovery. Then after discovering the neighbors the system will monitor the neighbor nodes by capturing the network packets. The neural network is trained with the past historical data and the weights are adjusted accordingly to get the desired output. Then the gathered packet related information is fed to the trained neural network to compute the trust value.
Then the recommendations about the selected node by the neighboring nodes are collected. Then the aggregated trust is formulated by summing up the direct trust value and the recommendations. The recommendations are weighted based on the relationship maturity.

Next step is to update the trust value of a node in the trust record by comparing the existing trust value with the defined threshold value. If the trust level of the node is lower than the threshold value then the trustworthiness of the node is said to be untrusting else it is set as trust worthy node.

When the node chooses to be in listen mode, it broadcasts the DISCOVER message in the first mini-slot and waits for the ACK in the second mini-slot. During third mini-slot it sends the confirmation to the receivers.

When the node chooses to be in listen mode, it receives the DISCOVER message in the second mini-slot and sends the ACK to the sender if it successfully receive the discover message. In the third mini-slot it receives the confirmation message from the sender.

Figure 3 Time slot structure used in scan based random algorithm.

In this algorithm, sender will experience the collision during the second mini-slot which means that sender has been discovered by more than one neighbor. So the sender will drop out itself for the next rounds of neighbor discovery.

C. TRUST COMPUTATION TECHNIQUE

The algorithm used for computing the trust of the neighbor nodes in the proposed system is relationship maturity based distributed trust management scheme. This algorithm used in the proposed system is distributed where every node computes the trust of every other node. It uses both direct trust and recommendation based trust for computing the trust.

To perform the weightage of the recommendation the proposed system uses the relationship maturity concept where the age of relationship is measured. The Nodes increase the weight of the recommendations coming from older neighbors and decrease the weight of recommendations coming from new neighbors. The trust computation formula used in the proposed system is as follows:

\[ T_A(B) = Q_A(B) + R(B) \]

Where \( T_A(B) \) is trust computed by A about B, \( Q_A(B) \) represents the direct trust compute by about B, \( R(B) \) is the aggregated recommendations about node B by all its neighbors.

The direct trust is computed by monitoring the network nodes using packet analyzers. The analyzer captures the packets of the neighbor nodes in the promiscuous mode and extracts the information required for trust computation. This information is fed to a trained neural network to compute the trust of the neighbor nodes.

The recommendations about the neighbors are received sing REP (Recommendation exchange protocol). REP is used to exchange the trust related information only between the neighbors. The recommendations are not forwarded throughout the network.

D. BACK PROPAGATION NEURAL NETWORK

The proposed system uses the BPNN (Back Propagation Neural Network) to train the neural networks for computing the trust. The BPN uses the supervised learning scheme to train the neural network. The BPN uses the set of input and their desired output to train the network. The input to train the BPNN is past historical data that are collected from the set of nodes. The weights to the hidden
layer are adjusted accordingly until the desired class arrives for the given input.

The number of layers used in BPNN is as follows:
- One input layer
- Two or more hidden layers
- One output layer.

The output layer’s result is fed back to the input layer and the weights are adjusted to eliminate the error/noise in the result.

The trace file collected by monitoring the network is used to train the Neural Network to classify the normal and abnormal behavior of the nodes. Once the NN is trained, it can be used to predict the trust level of the nodes.

V. EXPERIMENTAL SETUP

The proposed system is simulated using NS2 Simulator and MATLAB. The NS2 simulator is used to simulate the Neighbor discovery process. Each node is equipped with the directional antenna and the number of nodes in the network can be fixed approximately as 50. The following table describes the network configuration:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network size</td>
<td>250 nodes</td>
</tr>
<tr>
<td>Antenna Model</td>
<td>Directional Antenna</td>
</tr>
<tr>
<td>Transmission range</td>
<td>200m</td>
</tr>
<tr>
<td>Antenna beam width</td>
<td>30°</td>
</tr>
<tr>
<td>Discover packet size</td>
<td>20KB</td>
</tr>
<tr>
<td>ACK packet size</td>
<td>10KB</td>
</tr>
</tbody>
</table>

Table.1 Simulation Parameters

The NS2, packet analyzer module is used to analyze the flow monitoring trace file. This will generate the number of packets arrived, number of packets forwarded, number packets dropped and the movement of nodes for each node in the network. Then this information can be fed to the Neural Network to train the Back Propagation Neural Network.

The Neural Network Training and prediction is simulated using the MATLAB software. The dataset used for training the NN is the trace file collected by monitoring the network using packet analyzer.

The Back Propagation NN is used to train and predict the trust level of the nodes.

VI. CONCLUSION

The algorithms used to discover the neighbor nodes that are used in the existing system are Omni directional antenna based algorithm, directional antenna based algorithm and gossip based algorithm. These algorithms help to identify the neighbors but these algorithms do not provide the security architecture to identify the malicious or misbehaving nodes.

In the proposed system we integrate the trust based security system to the neighbor discovery process, in order to identify the malicious and selfishly behaving nodes. The proposed system aims to reduce the number of time slots required to discover all the neighbors in the network and also it provides security mechanism to improve the cooperation among the neighbor nodes. The trust among the neighbors is established to enhance the collaborative work among the neighbors. The proposed system exchanges the trust information about the nodes only with their neighbors thus it reduces the number of messages forwarded into the network and the data traffic in the network.

The proposed system aims to consume the lesser resource to convey the trust information among the neighbors.

REFERENCES


[5] Marco Fiore, Member, IEEE, Claudio Casetti, Member, IEEE, Carla-Fabiana Chiasserini, Senior Member, IEEE, Panagiotis Papadimitratos, Member, IEEE , “Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks”

[6] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, “ Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model “

