An Efficient Transmission of Data for MANETs Using Human Based Recommendation Exchange Protocol

R.Balaji (1), S.Kavin hari hara sudhan (2)

(1),(2) M.Tech student in Computer Science and Engineering
(1),(2) Dr.MGR Educational and Research Institute Chennai, Tamilnadu, INDIA
(1) mailmebalaji89@gmail.com
(2) mailmekavin.s@gmail.com

Abstract

This paper analyzes a trust model for mobile ad hoc networks. We provide nodes with a mechanism to build a trust relationship with its neighbors. The proposed model considers the recommendation of trustworthy neighbors and the experience of the node itself. In order to give trust value beyond the neighbor circle we are using Recommendation Exchange protocol (REP) which is used to give recommendation about neighbor’s neighbor. In existing, every node is having full details about entire nodes present in the Mobile ad hoc network but in our proposed system the individual node is not needed to maintain trust information of the entire network instead it can maintain information about the nodes in the radio range. By doing like this we can reduce the memory usage, computation power, resources, time constraints, etc. In addition, we introduce the RSA algorithm for security so we mitigate the effect of colluding attacks. We show the correctness of our model in a multi-hop network through simulations.

Index terms- Trust, MANETs, REP, Security

1. Introduction

Mobile Ad Hoc Network (MANETs) is a Collection of mobile nodes connected with wireless links. MANET has no fixed topology as the nodes are moving from one place to another place. All the nodes must co-operate with each other in order to route the packets. Cooperating nodes must trust each other. As a result, nodes must play the roles of router, server, and client, compelling them to cooperate for the correct operation of the network. This particular characteristic hinders applications and protocols conceived for conventional networks to perform efficiently in ad hoc networks. Therefore, new specific protocols for this type of network have been proposed and developed. However, the majority of the protocols and applications for ad hoc networks consider the perfect cooperation among all nodes. It is assumed, that all nodes behave in accordance with the specifications of the applications and protocols defined for the network. Nevertheless, this assumption may be false, due to resource restrictions or malicious behavior. Consequently, the nodes may not behave as expected by protocols or applications, causing the network to not work properly. Thus, the assumption that nodes behave correctly can lead to unforeseen pitfall, such as low network efficiency, high resource consumption, and a higher vulnerability to attacks. Therefore, a mechanism that allows nodes to infer the trustworthiness of other nodes is necessary.

A node should be capable of self-configuring, self-managing, and self-learning by means of collecting local information and exchanging information with its neighbors. Thus, it is important to communicate only with trustworthy neighbors, since communicating with misbehaving nodes can compromise the autonomy of ad hoc networks. We present a flexible trust model based on the concept of human trust and apply this model to ad hoc networks. Our Model builds, for each node, a trust relationship to all neighbors. The trust is based on previous individual experiences of the node and on the recommendations of its neighbors. The recommendations improve the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link outages.
The ability of assessing the trust level of its neighbors brings several advantages. First, a node can detect and isolate malicious behaviors, avoiding relaying packets to malicious neighbors. Secondly, cooperation is stimulated by selecting the neighbors with higher trust levels. Nodes learn based on the information exchanged with trustworthy neighbors to build a knowledge plane. In our model nodes interact only with its neighbors. As a result, nodes do not keep trust information about every node in the network. Keeping neighborhood information implies significant lower energy consumption, less processing for trust level calculation, and less memory space.

We introduce the concept of relationship maturity, which improves the efficiency of the trust evaluation process in the presence of mobility. Humans are able to know each other better as time goes by and the same idea applies here. Nodes increase the weight of the recommendations coming from older neighbors and decrease the weight of recommendations coming from new neighbors.

In this paper, we present a detailed description of our model, which includes the architecture and its components. The REP protocol scalability is evaluated, taking into account our implementation design and our results show an overhead reduction of almost 60% with roughly no impact at the convergence rate. Finally, we present a brief discussion about the results.

Even though we are maintaining trust between nodes which will only be useful for reducing resource usage. But to enhance the security level we are using RSA algorithm for encryption of data from sender to receiver.

**Trust: Definition**

According to Eschenauer et al., trust is defined as “a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities.” Trust has also been defined as the degree of belief about the behavior of other entities (or agents).

**Characteristics of Trust in MANETs**

Due to the unique characteristics of MANETs and the inherent unreliability of the Wireless medium, the concept of trust in MANETs should be carefully defined. The main features of trust in MANETs are as follows:

1. A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.
2. Trust should be determined in a highly customizable manner without excessive computation and communication load, while also capturing the complexities of the trust relationship.
3. A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, selfishness is likely to be prevalent over cooperation, for example, in order to save battery life or computational power.
4. Trust is dynamic, not static.
5. Trust is subjective.
6. Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
7. Trust is asymmetric and not necessarily reciprocal.
8. Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

**2. Trust Model**

The goal is to provide nodes with a mechanism to evaluate the trust level of its direct neighbors. Our model can be divided in two distinct layers as shown is Figure 1. The Learning layer is responsible for gathering and converting information into knowledge. The Trust layer defines how to assess the trust level of each neighbor using the knowledge information provided by the Learning layer and the information exchanged with direct neighbors. Both layers can interact with all layers of the TCP/IP model. In this paper, we focus on the Trust layer.

Trust layer defines how to assess the trust level of each neighbor using the knowledge information provided by the Learning plan and the information exchanged with neighbors. The proposed trust model components are shown in fig 2. In learning plane, the Behavior Monitor observes neighbors in order to collect information about their behavior it must be able to notice other nodes’ actions and transmit them.
to the Classifier. The Behavior Monitor also indicates the presence of new neighbors to the Recommendation Manager. The Classifier decides the quality of an action according to a previously defined classification. The Classifier then sends its verdict to the Experience Calculator. Experience Calculator estimates a partial trust value for a given node based on the information received by the Classifier.

The Recommendation Calculator computes all the recommendations for a given neighbor and determines a trust value based on the opinions of other nodes. This value is passed to the Trust Calculator component. The Trust Calculator evaluates the trust level based on the trust values received from the Experience Calculator (individual experiences) and the Recommendation Calculator (neighbor recommendations). The Trust Calculator also notifies the Recommendation Manager the need of sending a trust recommendation advertisement. The goal of the Auxiliary Trust Table is to supply nodes with additional information that improves the trust level evaluation.

2.1 Trust level evaluation

When a node first meets a new neighbor, it must assign an initial level of trust to this neighbor. This value depends on the network condition, level of mobility, time, and place. Afterwards, the trust level evaluation process begins with a trust recommendation request and the monitoring of the new neighbor. We define the trust level evaluation from node a about node b as a sum of its own trust and the contribution of other nodes, in the same way as defined by Virendra et al. [14]. The fundamental equation is

\[ T_a(b) = (1 - \alpha)Q_a(b) + \alpha C_a(b) \]  

Where

- \( \alpha \) = permits choosing the most relevant factor.
- \( Q_a(b) \) = represents the capability of a node to evaluate the trust level of their neighbors based on its own information.
- \( T_a(b) \) = Trust level evaluation from node a about node b
- \( C_a(b) \) = Aggregate value of the recommendation from all the neighbors

In order to obtain \( Q_a(b) \), we propose the following equation

\[ Q_a(b) = \beta E_T + (1 - \beta)T_a(b) \]  

Where \( E_T \) represents the value obtained by the judgment of neighbor actions, and the variable \( \beta \) allows choosing which factor is the more relevant at a given moment.
2.2 Contribution computation

The trust level calculation also considers the recommendation of direct neighbors. The set of recommendations is called contribution \( C_a(b) \) in Equation 1). Recommendation can be obtained by sending a Trust Request (TREQ) or by receiving a Trust Advertisement (TA) message from other neighbors. TA messages are unsolicited recommendations. A node only sends a TA message when the recommendation about a particular neighbor varies more than a certain threshold value. The contribution \( C_a(b) \) is defined as the sum of the recommendations from all nodes \( i \in K_a \) about node b weighted by the trust level of node a about node i, as follows

\[
C_a(b) = \frac{\sum_{i \in K_a} T_a(i) M_i(b) X_i(b)}{\sum_{j \in K_a} T_a(j) \sum_{j \in K_a} M_j(b)}
\]  
(3)

The group \( K_a \) defines the nodes from which recommendations will be considered. It is a subset of the neighbors of node a comprising all nodes that satisfy certain conditions. The contribution considers not only the trust level of others but also the accuracy and the relationship maturity. The accuracy of a trust level is defined by the standard deviation, similar to Theodorakopoulos and Baras [15]. The value in the trust level table of node a regarding node b is associated to a standard deviation \( \sigma_i(b) \), which refers to the variations of the trust level that node a has observed about node b. We use \( X \) as a random variable with a normal distribution to represent the uncertainty of the recommendation. It can be expressed as

\[
X_i(b) = N(T_i(b), \sigma_i(b))
\]  
(4)

The recommendation of node i about node b is weighted by \( M_i(b) \), Let \( M_i(b) \) be defined as the maturity of the relationship between nodes i and b, measured at node i. The relationship maturity is a measure of the time that two nodes have known each other. We use the relationship maturity to give more relevance to the nodes that know the evaluated neighbor for a long time.

In this paper we are using RSA Algorithm for Security.

Algorithm 3: RSA algorithm

**Key Generation:**

1. Select two prime no’s \( p \) & \( q \)
2. Calculate \( n \) as product of \( p \) & \( q \) is is th, i.e. \( n = pq \)
3. Calculate \( m \) as product of \( (p-1) \) & \( (q-1) \) i.e. \( m = (p-1) (q-1) \)
4. Select any integer \( e < m \) such that it is co-prime to \( m \), i.e. \( \text{gcd}(e,m) = 1 \)
5. Calculate \( d \) such that \( de \mod m = 1 \), i.e. \( d = e^{-1} \mod m \)
6. The public key is \( \{e,n\} \)
    The private key is \( \{d,n\} \)

**Encryption :**

- Plaintext = \( P \) & \( P < n \)
- Ciphertext = \( C \) & \( C = P^e \mod n \)

**Decryption :**

- Ciphertext = \( C \)
- Plaintext = \( P \) & \( P = C^d \mod n \)

3. Results

This section presents the results. First we expose the results of our model and show the effectiveness of the relationship maturity parameter. The mean value of the time between two actions performed by a node is set to 5 units of time. All results are presented with a confidence interval of 95%.

3.1 Performance on Multi hop Mobile Ad Hoc Networks

Our main goal with this experiment is to evaluate the trust system performance in mobile multi hop networks. We are also interested in analyzing the impact of the relationship maturity and the influence of the variation of parameters \( \alpha \) and \( \tau \). All figures present the trust level error (TLE) as a function of time, as in the previous section. The simulation scenario consists of 21 nodes with 250 m transmission range, which are placed in a 1000 m x 400 m area, as shown in Fig. 9. The distance between nodes is 150 m. We defined the first trust assignment equals to 0.9 for every node in the simulation. We also assume \( \alpha = 0.5 \). These are the standard values for the simulations.
3.2 Delay

This the graph for delay calculation in which X axis is considered to be a Frequency and Y axis is considered to a Time. Here Red line denotes a performance of existing system and Green line denotes a performance of proposed system. So it’s obvious that the proposed system getting very delay when comparing with the existing system. In the existing system delay will be above 75% but in proposed system it is less than 12%. So our proposed system performance wise better than existing one.

3.3 Throughput

This the graph for throughput calculation in which X axis is considered to be a Frequency and Y axis is considered to a Time. Here Red line denotes a performance of existing system and Green line denotes a performance of proposed system. So it’s obvious that the proposed system getting very delay when comparing with the existing system. In the existing system throughput will be above 26% but in proposed system it is less than 6%. So our proposed system performance wise better than existing one.

4. Conclusion

This paper analyzes a trust model for mobile ad hoc networks. We aim at building a trust relationship among nodes. We propose a flexible trust model based on the concept of human trust, which provides nodes with a mechanism to evaluate the trust level of its neighbors. We provide a mechanism for nodes to evaluate the trust level of their neighbors. We analyze through simulations the performance of the proposed model in a mobile multihop network. We also propose the Recommendation Exchange Protocol (REP) which enables nodes to send and receive recommendations. We perform a number of simulations to evaluate the performance of the Recommendation Exchange Protocol and show its scalability. We show that our implementation of the REP protocol can significantly reduce the number messages.
Future work includes defining and implementing a monitoring scheme for a specific application and applying our model to improve the service/application performance, as for instance, an authentication protocol.

References


Authors Profile

(1) Author R.Balaji is an M.Tech student in computer science & engineering, Dr.MGR University, Chennai, Tamil Nadu, and India. He has published 1 paper in international conference and 2 papers in national conferences. He shall be contacted through mailmebalaji89@gmail.com

(2) Author S. Kavin Hari Hara Sudhan is an M.Tech student in computer science & engineering, Dr.MGR University, Chennai, Tamil Nadu, India. He has published 1 paper in international journal,1 International conference and 3 papers in national conferences. He shall be contacted through mailmekavin.s@gmail.com