A Power Efficient Trust Based SecureRouting Scheme for Mobile Ad-Hoc Networks

MV Rathnamma*[1], P Chenna Reddy[2]
JNTUA, Anantapur-AP-India. Tel::+91 9849777831
JNTUCEP, Pulivendula-YSR-AP-India
*Corresponding author, e-mail: mvrathnamma@gmail.com[1], pcreddy1@rediffmail.com[2]

Abstract

MANETs are self-organizing, infrastructure less ad-hoc networks with many challenges like low power, limited storage and limited processing devices. Among all the parameters that affect the network efficiency accuracy, scalability, and power consumption are main challenges in the routing of Mobile ad-hoc networks. The network lifetime is dependent on the power efficiency of the nodes in the network. The protocols have to provide the energy efficient route through intermediate nodes in the network. The trust based routing approach is one of the best mechanisms to establish an energy efficient route between source and destination. In this paper we first propose the family relationship based trust model and then propose a new energy efficient trust based routing protocol to reduce the routing overhead, delay and provides better packet delivery ratio that performs better than the existing routing protocols.

***Keywords**: Mobile ad-hoc networks, Security, Trust Management*

1. Introduction

The MANETs are autonomous system of portable wireless mobile nodes that communicate without any specific infrastructure or centralized access. Every mobile node in the network acts as a router and works as an intermediate node between source and destination. Many Reactive, Proactive and hybrid routing protocols have been proposed to make proper communication in the network nodes. In MANETs, node communication is dependent on the mutual trust [1] [2] among the nodes. The constraints in the MANETs pose many new research challenges in the routing, privacy, trust and security including authentication and key management among the nodes.

A Genetic algorithm based energy entropy multipath routingapproachwas proposedin [16] to adjust energy utilization of individual node, calculate the minimal energy of node and drag out the lifetime and energy change of the system. The energy saving routing protocols have been designed to improve the performance in terms of overhead in routing, end to end delay, PDR of the networks and consumption of the energy. Security is one of the main challenges for the practical implementation of ad-hoc networks, such as MANETs or Wireless sensor networks. Traditionally, functions that drive WSNs, such as medium accesscontrol (MAC) and routing protocols, always assume that theoperating environment is trustworthy [15]. This assumption is not always right and remote environments are always susceptible to attacks and are very tough to protect. It is observed that the energy inefficiency affects the overall network performance and lifetime. So we can say that the insufficient power of a node leads to link failures and degrades the network performance.

The concept of trust originally taken from social sciences and is described as subjective belief about the behaviors of a particular entity [3]. Trust management is introduced [4] and clarified as "trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships." The design of trust based energy efficient routing protocol in this paper, first explains about the energy model to find the energy factor and gives a overview of our trust based approach to be implemented.

The remaining part of the paper organized as follows: In section 2, the background and related work is given. Section 3 describes the overview of trust and reputation model used in this method. Section 4 shows our research framework and proposed routing protocol. In Section 5, extensive experiments and simulations conducted in comparison with the existing protocols is

Received January 21, 2016; Revised April 14, 2016; Accepted April 28, 2016

presented, and finally in section 6, conclusion and challenges encountered and future scope is presented.

2. Background Work

For efficient utilization of battery power of nodes in the network, various power efficient routing mechanisms [5]-[11] have been proposed. Trust values are used to construct safe paths among the nodes in the network. Considerable amount of work is done on the power efficient routing protocols but not in trust based approach. Authors [12] proposed a new energy efficient and secure SEER multipath routing protocol. This protocol updates each node with remaining energy on dynamic basis for finding the appropriate path from multiple choices. The main advantage of this kind of approach is minimizing the overhead to maintain the route and can maximize the efficiency and lifetime of other nodes in the network.

Many authors have discussed various issues regarding trust management in MANET's and in wireless sensor networks. The authors in [13] have discussed a novel trust aware routing protocol that uses direct trust and indirect trust. It has monitoring component with several metrics like data confidentiality, data integrity, available energy, network-ack, and reputation. A TCLM [14], trust based cross layer model uses the ACKs from DL layer and TCP to promote trust and eliminates the malicious nodes and insists highly trusted route from source to destination.

Trust management in MANETs is needed when new nodes join the network and wants to establish a communication with acceptable level of trust relationships among themselves. Trust management has applicability in many decision making situations including intrusion detection, access control, key management, authentication and for effective routing. Trust management, includes trust establishment and trust revocation.

3. Trust Evaluation

In our earlier work, we proposed trust based model for MANETs using Family relationship based approach. The misbehavior of the nodes degrades the performance of the network, so the trust module used to provide secure communication and efficient routing is possible. A mobile ad-hoc network fully depends on the co-operation between nodes for routing and forwarding. The successful delivery of data from source to destination will happen if all the nodes co-operate well. The attacksare identified and solved by intrusion detection, secure routing, key management and trust management.This section discusses about the different ways of establishing trust between nodes in mobile ad-hoc networks.

Direct Trust

The direct trust will be calculated by direct interaction between immediate neighboring nodes in the network as shown in Figure 1. The direct trust can log the number of successful packet transfers, recommendation and misbehavior detection. It is the most widely used trust calculation method when there are no pre-established infrastructures and centralized control.

Recommendation Trust

There might be some malicious nodes, which behave differently with different nodes. In this kind of situation, the direct trust is not sufficient and so the recommendation about that particular node will also be considered to calculate trust. Here the other mutual neighbors will share its trust table with the neighbor nodes. The trust calculation method is known as recommendation trust or indirect trust. There are some problems in this recommendation trust, such as false recommendation by the other nodes due to malicious nature of network nodes.

Trust Computation

In this sub section we discuss about the different trust computations used in our work. All trust values computed in our scheme ranges from 0 to 1. Based on the total trust value the role/relationship will be assigned to the neighbor node. For calculating trust, we are using the concept of convex hull which gives a value that lies between two fixed points.

Initial Trust

This trust is calculated using the parameters, battery power and signal strength. This is the basic criteria for a node to be in the network. This trust is the main factor to decide whether to keep the node as a neighbor or not. Trust upgradation also depends on this trust value. Initial trust value is mainly used to reduce the attacks by the selfish nodes because of resource limitation.

$$IT(N) = (\rho * BP) + (\sigma * SS)$$

In above equation *IT*represents the initial trust, *BP* represents the battery power and *SS* represents the signal strength of neighbors of new node *N*. The ρ and σ represents the variables and the summation should be 1. In our work we have taken 0.5, 0.5 for ρ and σ respectively.

Behavioral Trust

The behavioral trust is calculated by direct interaction and experience of one node to another node. The parameters for calculating behavioral trust will vary for different nodes based on its level as mentioned in table 1.

$$BT(N) = \frac{1}{l} * \sum_{i=1}^{l} p_i$$

In the above equation *BT* represents the behavioral trust, *l*represents the trust level and *p*represents the parameter of Node *N*. For example if the node level is *l*= 2, the p_1 and p_2 of node *N* will be taken as shown in Table 1.

$$RT(N) = \frac{1}{n} * \sum_{i=1}^{n} t_i$$

Recommendation Trust

The recommendation trust is calculated from the mutual neighbors of any two neighboring nodes. All the mutual neighbors will share their trust value or opinion about a particular node to calculate the recommendation trust.

In the above equation, *RT* represents recommendation trust, *n* represents the number of mutual neighbors and t_i represents the trust value shared by i^{th} mutual neighbor of node *N*.

Total Trust: The total trust is calculated from Behavioral trust and recommendation trust. The total trust will be useful in upgrading or degrading the trust level of a node. The total trust also ranges from 0 to 1.

$$TT(N) = \left(\propto * BT(N)\right) + (\beta * RT(N))$$

In the above equation, *TT* represents total trust, *BT* represents behavioral trust and *RT* represents a recommendation trust of node *N*. The variables α and β should have the values such that the summation will be 1. In our work we consider 0.7 and 0.3 for α and β respectively.

4. Algorithm and Proposed Work

This section describes about the key idea of our proposed work. There are two different phases namely bootstrapping and upgrading/downgrading phase. The bootstrapping phase will take place when a new node wants to join the network without any previous experience. In Bootstrapping phase initial trust is used for trust computation. The upgrading/downgrading phase will be used to update the trust value and relation of the neighbor nodes.

4.1. Boot Strapping Phase

When a new node wants to join the network, the neighbor will check whether any mutual neighbors are there or not. If any mutual neighbors are there, the node will request for recommendation trust from all other mutual neighbors having relationship more than or equal to "parent". Then the new node will be added to the network one level lesser than the recommendation trust. If not, the initial trust will be calculated and the node will be added to the network with least privilege. The working of bootstrapping phase is described in following algorithm:

Algorithm 1 (Bootstrapping phase):

```
// When new node wants to be a neighbor
if (mutual neighbor) {
        calculate recommendation trust RT(N)
        add node N as a neighbor (trust value = RT(N)/2)
}
else {
        calculate initial trust IT(N)
        add node N as a neighbor (trust value = 0)
}
```

4.2. Upgrading/Downgrading Phase

When a node wants more privilege, it will send an update request to its neighbor. First initial trust is calculated to ensure that the node is having sufficient resources. If the node has sufficient resources, total trust is calculated from behavioral trust and recommendation trust. If the total trust is greater than threshold value 0.75 then it is eligible for up-gradation. Otherwise, it indicates the malicious behavior; then the node is marked as malicious node by setting the trust value to -1. If there are no sufficient resources, but the total trust is more than 0.75; then the node is not eligible for upgradation. In this case the node will retain its old trust value. The following algorithm explains the actual working of upgrading/downgrading phase.

Algorithm 2 (Upgrading / Downgrading Phase):

```
// When a trust upgrade request from node N
calculate initial trust of node N [IT(N)]
if (IT(N)>0.75) {
calculate total trust of node N [TT(N)]
if (TT(N)>0.75) {
upgrade node N (trust value = current trust *2)
}
else
mark node N as malicious node (trust value = -1)
}
else {
if (TT(N)>0.75) {
Don't upgrade node N (trust value = current trust)
}
else
mark node N as malicious node (trust value = -1)
}
```

4.3. Energy Saving Model

From trusted energy saving perspective, power aware routing protocol PTSRP, based on the above described trust method for efficient utilization of energy and uses hybrid power saving scheme, which is more balanced and secure is proposed. It provides better sharing of network resources and maintains efficient power saving. This is achieved by isolating the bad nodes and delegating part of the trust calculations to the senders as base stations.

To illustrate the benefits of PTSRP, we will show the calculations for above approach with respect to the power. The overhead is classified to two different parts, the reports sent by the nodes and central report sent by the BS.

$$\text{Energy 1} = M \times N \times AN \times [(h-1) \times Rx + h \times Tx] \quad (1)$$

Here
M - Size of the message, per neighbor in bytes.
N - Total nodes in the network.
h- Average number of hops from node to BS.
AN- Active neighbors of a node.
Rx energy- Energy to receive one byte
Tx energy- Energy to transmit one byte
As per the BS central report, it consists of messages from all malicious nodes and is broadcasted to all the nodes for every time period t is calculated as follows

$$\text{Energy 2} = M \times N \times Ml \times (Rx + Tx) \quad (2)$$

Where Ml is the number of malicious nodes. Assume tx=E and normalizing Rx we obtain,

$$e1 = M \times N \times AN \times [(E+1) \times h - 1] \quad (3)$$

$$e2 = M \times N \times Ml \times (E+1) \quad (4)$$

If the average time interval of dropping packets is td

$$Einc = 2 \times \varphi \times B \times [Tx \times H \times P + Rx \times (H-1) \times P] \quad (5)$$

where
$\varphi$is the packet size in bytes
Packet follows the full duplex communication and dividing by Rx to normalize, we obtain

$$Einc = 2 \times \varphi \times B \times [(E-1) \times H \times Ps] \quad (6)$$

The energy saving can be obtained for the frequent periods τ is calculated as

$$Es = Einc \times \tau / tdrop / e1 + e2 \quad (7)$$

Es is considered as the energy savings for the PTSRP and all the values are filtered results of trust from the previous section algorithms.

5. Results and Analysis

In this section, we design some simulation test experiments of PTSRP protocol using Network Simulator-2. In this simulation test experiments, we simulate and compare energy cost and total receiving data packets against the other proposed protocols like SAODV [17] and TRRP [18].

5.1 Performance Evaluation

Total Throughput: The total number of packets received per unit time.
Total Overhead: Total number of routing control packets transmitted at time *t* by all the nodes in the network.
Packet Delivery Ratio: It is the ratio of total number of packets successfully delivered to the total number of packets sent.
Packet latency: the total time elapsed since a data packet is transmitted to time the data packet reached the destination.
The simulations are conducted to examine the performance by adding security. Here PTSRP is compared to SAODV and TRRP.

Table 1. Simulation Parameters

Number of Nodes	100
Topology dimension	1000m x 1000m
Radio range	250m
Node pause times	0-40s
Traffic Pattern	FTP/TCP`
Maximum node speed	1-20m/s
Source-destination pairs	20

In our scenario, simulations conducted to examine the performance by adding security to the routing protocols. We compare our proposed model with existing two routing protocols and obtain better results. Simulation parameters are given in the table, and a malicious node randomly drops data packets and can be detected during formation of network topology. Here the dropping is in the scale of 20% to 50% and each simulation time is 600s to collect the output data.

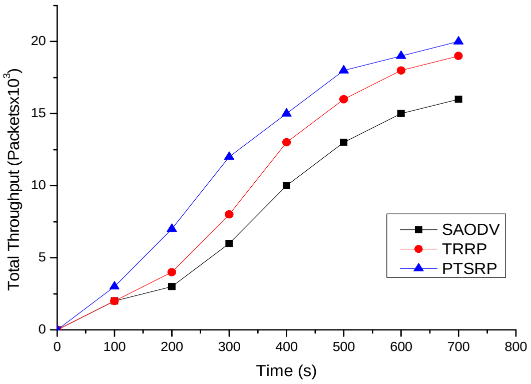

Figure 1. Total Throughput in the presence of 5 malicious nodes

Figure 1 represents the throughput of the three protocols under five malicious nodes out of 50. All the routing protocols are delivering the packets to the destinations due to less number of malicious nodes. However, our proposed method outperforms the others, hence the efficient results.

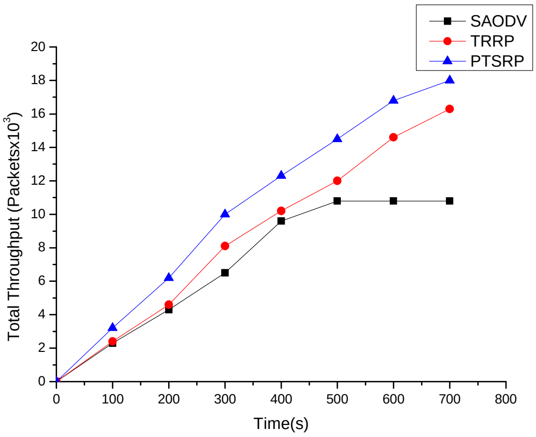

Figure 2. Total Throughput in the presence of 10 malicious nodes

If the number of malicious nodes increases from 5 to 10, and to 20, as shown in the Figure 2 and Figure 3, we can observe the packet delivery of TRRP and SAODV decreases proportionally, whereas PTSRP still delivers the packets efficiently. SAODV stops delivering of packets at time t=540 in the 30% to 40% malicious nodes. Due to the heavy packet drop, the connection will be timed out and new route discovery will be initiated again. Even more number of malicious nodes in the network, PTSRP discovers the trustworthy routes and results successful packet delivery.

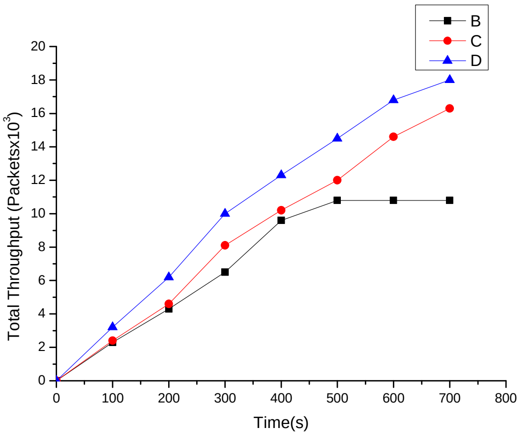

Figure 3. Total Throughput in the presence of 20 malicious nodes.

Figure 4 represents the total overhead of SAODV, TRRP and proposed PTSRP. From the analysis of the results, PTSRP has the less overhead than the remaining routing approaches. The basic reason behind this is that the PTSRP detect the malicious nodes using trust based mechanism and avoids those nodes from the routing. SAODV tends to wait and time out often.

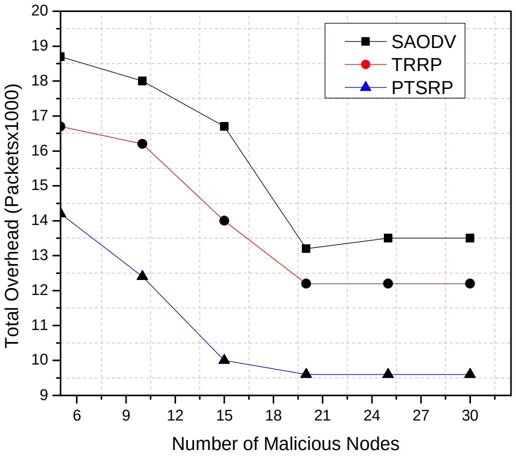

Figure 4. Total overhead in the presence of malicious nodes

Figure 5 shows the PDR of PTSRP at different speeds compared to the TRRP and SAODV. PTSRP chooses the more reliable routes by avoiding the more malicious nodes and increases the efficiency. The speed increases from 1.3 to 2.6 m/s, even though link breakages may reduce the packet delivery ratio, the nodes are more likely to find the available pairs to forward the packets.

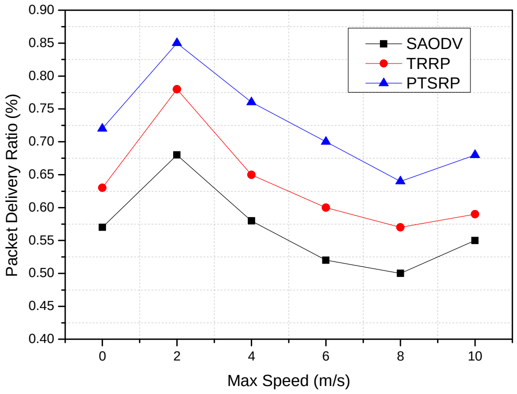

Figure 5. Packet Delivery Ratio at different speeds

As the maximum speed increases from 2.5 to 10 m/s, the link breakage is main cause that reduces the packet delivery ratio. PDR decreases as the maximum speed increases.

6. Conclusions and Future Work

From the results of simulations, we summarize the contribution of this research; PTSRP is suitable for the secure routing with trusted values in MANETs due to it's considerable accuracy, average path length and moderate energy consumption. This paper proposed a method for trust calculation, and the trust mechanism integrated with the efficient power utilization model and gives the better results than widely used AODV routing scheme. The proposed PTSRP outperforms the existing routing protocols in the performance. Still it is possible to improve the energy saving scheme by reducing calculation overhead of trust.

References

[1] JH Cho, A Swami, and IR Chen. “A Survey on Trust Management for Mobile Ad Hoc Networks”. *IEEE Communications Surveys & Tutorials*. 2011; 13(4).

[2] L Capra. “*Toward a Human Trust Model for Mobile Ad-hoc Networks*”. Proc. 2nd UK-UbiNet Workshop, Cambridge University, Cambridge, UK. 2004.

[3] KS Cook (editor). *Trust in Society*. Russell Sage Foundation Series on Trust, New York. 2003; 2.

[4] M Blaze, J Feigenbaum and J Lacy. “*Decentralized Trust Management*”. Proc. IEEE Symposium on Security and Privacy. 1996: 164 - 173.

[5] D Feng and Y Zhu. “An Improved AODV Routing Protocol Based on Remaining Power and Fame”. *Electronic Computer Technology*. 2009: 117-121.

[6] V Rodoplu and TH Meng. “Minimum Energy Mobile Wireless Networks”. *IEEE Journal on Selected Areas in Communications.* 1999; 17(8): 1333-1343.

[7] PJ Wan, G Calinescu, XY Li and O Frieder. “Minimum-energy broadcasting in static ad hoc networks”. *Wirel. Netw. Journal*. 2002; 8(6): 607-617.

[8] I Park, TH Meng and I Pu. “Blocking Expanding Ring Search Algorithm for Efficient Energy Consumption in Mobile Ad Hoc Networks”. *IFIP WONS*. 2006: 191-195.

[9] LM Feeney and M Nilsson. “Investigating the Energy Consumption of a Wireless Network Interface in Ad hoc Network Environment”. *IEEE INFOCOM*. 2001; 3: 1548-1557.

[10] N Sumathi and AS Thanamani. “Evaluation of Energy Efficient Reactive Routing rotocols in QoS Enabled Routing for MANETS”. *Int. Journal of Computer Applications*. 2011; 14: 10-14.

[11] A Syarif and RF Sari. “Performance Analysis of AODV-UI Routing Protocol with Energy Consumption Improvement under Mobility Models in Hybrid Ad hoc Network”. *Int. Journal on Computer Science and Engineering (IJCSE).* 2011; 3: 2904-2918.

[12] N Nasser and Y Chen. “SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks”. *Computer Communications*. 2007; 30(11-12): 2401–2412.

[13] Theodore Zahariadis, Panagiotis Trakadas, Helen Leligou, Panagiotis Karkazis. “*Implementing a Trust-Aware Routing Protocol in Wireless Sensor Nodes*”. DeSE 2010, London UK. 2010.

[14] Rahhal HA, Ali IA, Shaheen SI. "A novel Trust-Based Cross-Layer Model for Wireless Sensor Networks". 28th *National Radio Science Conference (NRSC)*. 2011; 1(10).

[15] G Theodorakopoulos and J Baras. “On trust models and trust evaluation metrics for ad hoc networks”. *IEEE J. Sel. Areas Commun*. 2006; 24(2): 318 – 328.

[16] B Sun, C Gui, and P Liu. “*Energy Entropy Multipath Routing Optimization Algorithm in MANET based on GA*”. Proc. Fifth IEEE Int. Conf. on Bio-Inspired Computing: Theories and Applications (BIC-TA). 2010: 943-947.

[17] MG Zapata and N Asokan. “Securing Ad hoc Routing Protocols”. WiSe. 2002.

[18] Neelakandan S, Anand JG. "Trust based optimal routing in MANET's". *Emerging trends in Electrical and Computer Technology (ICETECT*. 2011: 1150, 1156.