International Journal of Soft Computing 12 (4): 247-252, 2017
ISSN: 1816-9503

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

M.V. Rathnamma and P. Chenna Reddy
Department of CSE, JNTU University, Anantapur, Andhra Pradesh, India

Abstract: MANETs are self-organizing infrastructure less ad-hoc networks with many challenges with 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 must 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 study, 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 outperforms the existing routing protocols.

Key words: Mobile ad hoc networks, security, trust management, existing, efficiency

INTRODUCTION

The MANETs are autonomous system of portable wireless mobile nodes 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 has been proposed to make proper communication in the network nodes. MANETS node communication is highly depends on the mutual trust (Cho *et al*., 2010; Capra, 2004) 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 routing approach proposed (Sun *et al*., 2010) 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 Access Control (MAC) and routing protocols always assume that the operating environment is trustworthy (Theodorakopoulos and Baras, 2006). This assumption is not always right and remote environments always susceptible to attacks and very tough to protect. It 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 (Cook, 2003). Trust management is introduced (Blaze *et al*., 1996) 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 study we first explains about the energy model to find the energy factor and gives a overview of our trust based approach to be implemented.

Literature review

Background work: For efficient utilization of battery power of nodes in the network, various power efficient routing mechanisms (Feng and Zhu, 2009; Feeney and Nilsson, 2001; Park *et al*., 2006; Rodoplu and Meng, 1999; Syarif and Sari, 2011; Wan *et al*., 2002; Sumathi and Thanamani, 2011) have been proposed. Trust values used to construct safe paths among the nodes in the network. Considerable amount of work done on the power efficient routing protocols but not in trust based approach. Nasser and Chen (2007) proposed a new energy efficient and secure SEER multipath routing protocol. This protocol updates the 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.

Corresponding Author: M.V. Rathnamma, Department of CSE, JNTU University, Anantapur, Andhra Pradesh, India

Many researchers have discussed various issues regarding trust management in MANET's and in wireless sensor networks. The researcher Zahariadis *et al.* (2010) 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, reputation. A TCLM (Rahhal, 2011) 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 needed when new nodes join in the network and wants to establish a communication with acceptable level of trust relationships among themselves. Trust management in has applicability in many decision making situations including intrusion detection, access control, key management, authentication and for effective routing. Trust management including trust establishment and trust revocation.

MATERIALS AND METHODS

Trust evaluation: In our earlier research, 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 attacks 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 Fig. 1. The direct trust can log the number of successful packet transfer recommendation and misbehavior detection. It is the most widely used trust calculation method when there no pre-established infrastructure and centralizer.

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.

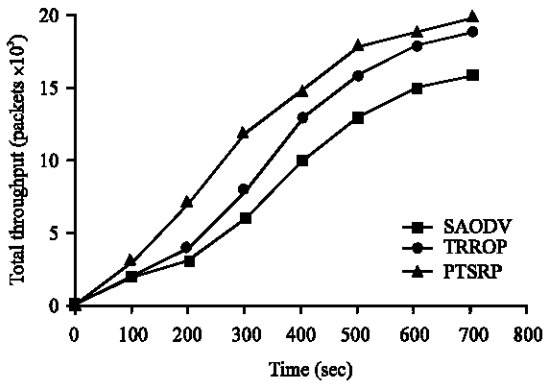

Fig. 1: Total throughput in the presence of 5 malicious nodes

Trust computation: In this study, we discuss about the different trust computations used in our work. All trust values computed in our scheme ranges from 0-1. 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 up gradation also depends on this trust value. Initial trust value is mainly used to reduce the attacks by the selfish nodes because of resource limitation:

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

Where:

IT = The initial trust
BP = The battery power
SS = The signal strength of neighbors of new node N

The ρ and σ represents the variables and the summation should be 1. In our research, we have taken 0.5, 0.5 for ρ and σ, respectively.

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

Table 1: Simulation parameters

Varibles	Values
No. of nodes	100
Topology dimension	1000×1000 m
Radio range	250 m
Node pause times	0-40 sec
Traffic pattern	FTP/TCP`
Maximum node speed	1-20 m/sec
Source-destination pairs	20

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

Where:
BT = The behavioral trust
l = The trust level
p = 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.

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

Where:
RT = Recommendation trust
n = The number of mutual neighbors
t_i = The trust value shared by ith mutual neighbor of node N

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.

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 0-1:

$$TT(N) = (\alpha \times BT(N)) + (\beta \times RT(N))$$

Where:
TT = Total trust
BT = Behavior trust
RT = A recommendation trust of node N

The variables a and b should have the values such that the summation will be 1. In the study, we consider 0.7 and 0.3 for a and b, respectively.

Algorithm and proposed work: This study describes about the key idea of our proposed research. 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.

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)
}
```

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 making the trust value to -1. If there are no sufficient resources, but the total trust is >0.75; then the node is not eligible for up gradation. 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)
}
```

Energy saving model: From trusted energy saving perspective the proposed, 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. It provides the better sharing of network resources and maintains efficient power saving. This process achieved by isolating the bad nodes and delegating part of the trust calculations to the senders as base stations.

To shown 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:

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

Where:

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:

$$\text{Energy}2 = M \times N \times M1\,(Rx + Tx) \quad (2)$$

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

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

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

If the average time interval of dropping packets is t_d:

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

where, φ is the pocket size in bytes. Packets follows the full duplex communication and dividing by Rx to normalize we obtain:

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

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.

RESULTS AND DISCUSSION

In this study, 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 (Zapata and Asokan, 2002) and TRRP (Neelakandan and Anand, 2011).

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 and reached to the destination. The simulations are conducted to examine the performance by adding security. Here, PTSRP is compared to SAODV and TRRP. 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 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 20-50% and each simulation time 600 sec to collect the output data.

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.

If the number of malicious nodes increases from 5-10 and to 20 as shown in the Fig. 2 and 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 30-40% malicious nodes. Due to the

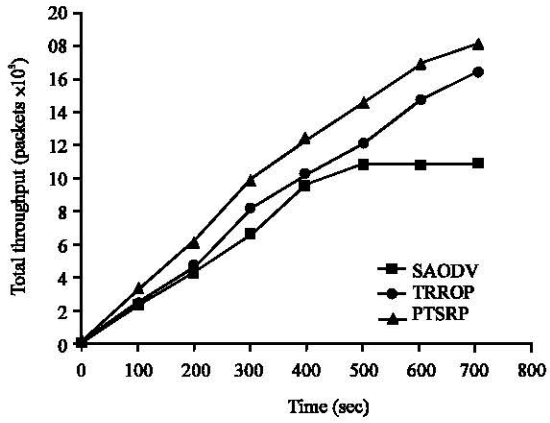

Fig. 2: Total throughput in the presence of 10 malicious nodes

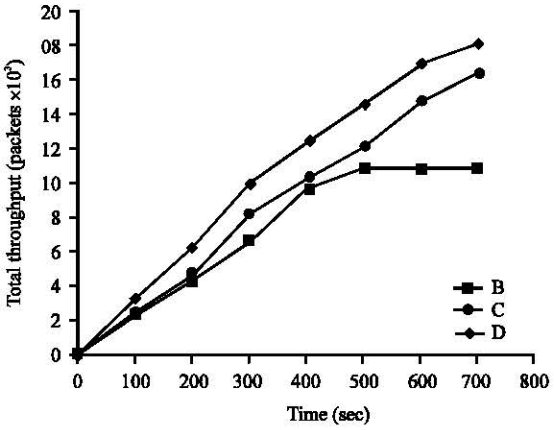

Fig. 3: Total throughput in the presence of 20 malicious nodes.

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 (Fig. 3).

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.

In Fig. 5, it shows that 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 1.3-2.6 m/sec even though link breakages may reduces the packet delivery ratio, the nodes are more likely to find the available pairs to forward the packets.

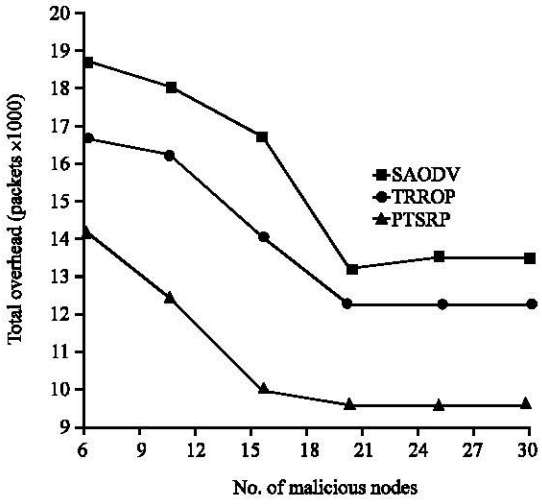

Fig. 4: Total overhead in the presence of malicious nodes

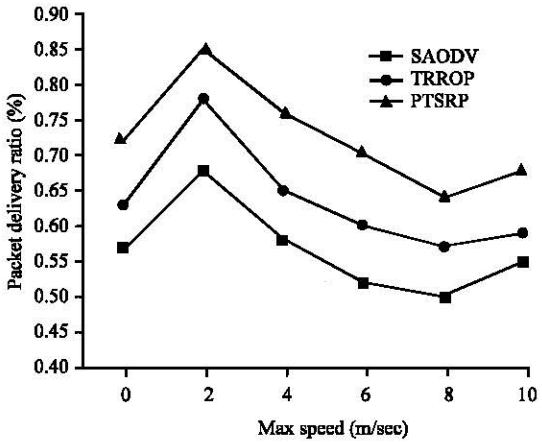

Fig. 5: Packet delivery ratio at different speeds

As the maximum speed increases from 2.5-10 m/sec the link breakage is main cause that reduces the packet delivery ratio. The PDR decreases the maximum speed increases.

CONCLUSION

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 study 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

Blaze, M., J. Feigenbaum and J. Lacy, 1996. Decentralized trust management. Proceedings of the IEEE Symposium on Security and Privacy, May 6-8, 1996, Oakland, CA., USA., pp: 164-173.

Capra, L., 2004. Toward a human trust model for mobile ad-hoc networks. Proceedings of the 2nd Workshop on UK-UbiNet, May 5-7, 2004, Cambridge University, Cambridge, UK., pp: 1-2.

Cho, J.H., A. Swami and I.R. Chen, 2010. A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 13: 562-583.

Cook, K.S., 2003. Trust in Society. Vol. 2, Sage, New York, USA.,.

Feeney, L.M. and M. Nilsson, 2001. Investigating the energy consumption of a wireless network interface in an Ad Hoc networking environment. Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies, April 22-26, 2001, Anchorage, AK, USA., pp: 1548-1557.

Feng, D. and Y. Zhu, 2009. An improved AODV routing protocol based on remaining power and fame. Proceedings of the International Conference on Electronic Computer Technology, February 20-22, 2009, IEEE, Macau, China, ISBN: 978-0-7695-3559-3, pp: 117-121.

Nasser, N. and Y. Chen, 2007. SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. Comput. Communi., 30: 2401-2412.

Neelakandan, S. and J.G. Anand, 2011. Trust based optimal routing in MANET's. Proceedings of the 2011 International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), March 23-24, 2011, IEEE, Tamil Nadu, Indian, ISBN: 978-1-4244-7923-8, pp: 1150-1156.

Park, I., J. Kim and I. Pu, 2006. Blocking expanding ring search algorithm for efficient energy consumption in mobile ad hoc networks. Proceedings of the 3rd Annual Conference on Wireless on demand Network Systems and Services (WONS 2006), January 30, 2006, IFIP, New York,USA., pp: 191-195.

Rahhal, H.A., I.A. Ali and S.I. Shaheen, 2011. A novel trust-based cross-layer model for wireless sensor networks. Proceedings of the 28th National Conference on Radio Science (NRSC), April 26-28, 2011, IEEE, Cairo, Egypt, ISBN:978-1-61284-805-1, pp: 1-10.

Rodoplu, V. and T.H. Meng, 1999. Minimum energy mobile wireless networks. Selected Areas Commun., 17:1333-1344.

Sumathi, N. and D.A.S. Thanamani, 2011. Evaluation of energy efficient reactive routing protocols in QoS enabled routing for MANETS. Intl. J. Comput. Appl., 14: 10-14.

Sun, B., C. Gui and P. Liu, 2010. Energy entropy multipath routing optimization algorithm in MANET based on GA. Proceedings of the IEEE 5th International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), September 23-26, 2010, IEEE, Changsha, China, ISBN:978-1-4244-6437-1, pp: 943-947.

Syarif, A. and R.F. Sari, 2011. Performance analysis of AODV-UI routing protocol with energy consumption improvement under mobility models in hybrid ad hoc network. Intl. J. Comput. Sci. Eng., 3: 2904-2918.

Theodorakopoulos, G. and J.S. Baras, 2006. On trust models and trust evaluation metrics for ad hoc networks. IEEE J. Selected Areas Commun., 24:318-328.

Wan, P.J., G. Calinescu, X.Y. Li and O. Frieder, 2002. Minimum-energy broadcasting in static ad hoc wireless networks. Wirel. Netw., 8: 607-617.

Zahariadis, T., P. Trakadas, H. Leligou, P. Karkazis and S. Voliotis, 2010. Implementing a trust-aware routing protocol in wireless sensor nodes. Proceedings of the Conference on Developments in E-systems Engineering (DESE), September 6-8, 2010, IEEE, London, UK., ISBN:978-1-4244-8044-9, pp: 47-52.

Zapata, M.G. and N. Asokan, 2002. Securing ad hoc routing protocols. Proceedings of the 1st ACM Workshop on Wireless Security, September 28, 2002, Atlanta, GA., USA., pp: 1-10.