International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 4, August 2014, PP 63-74
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Knowledge Based Trust for Secure Routing Process in Mobile Ad-hoc Networks

K.S.Charumathi
M.E. Student, PIIT/Mumbai University
Mumbai, Maharashtra, India
ks.charumathi@yahoo.co.in

Dr. Madhumita Chatterjee
CSE department, PIIT/Mumbai University
Mumbai, Maharashtra, India
c_a_mita@yahoo.com

Abstract: *In recent years, there has been a huge use of mobile computing devices and those led to the development of ad-hoc networking standards and provide the mobile nodes to set up self-organizing, adaptive, and short-lived networks. A mobile ad hoc network consists of wireless mobile nodes forming a temporary network without the help of centralized infrastructure, and where nodes communicate through multi-hops. Trust should be derived under time-critical conditions, and in a distributed way. Trust management in MANETs is needed when participating nodes establish a network, without any interactions previously, with an acceptable level of trust themselves. Trust system can be used to provide network security services like access control, malicious node detection, secure resource sharing, and authentication. So, evaluate the trust value of the nodes periodically based on trust metrics and computational methods. Trust management and computations are challenging issues in MANETs due to independent movement of nodes and computational complexity constraints. Trust management is a multifunctional control mechanism in which the most important task is to establish trust between nodes who are neighbors and making a routing path. A key concept of this project is to propose a trust based secure routing process scheme in MANETs without using any centralized infrastructure. We designed a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. The proposed scheme minimizes the overhead using transiting packets on the network to update nodes knowledge about other nodes trustworthiness and select a secured routing path based on trust knowledge of nodes.*

Keywords: *Trust, Trust Management, Secure Routing, Direct Trust, Indirect Trust.*

1. INTRODUCTION

MANETS do not rely on extraneous hardware, which makes them an ideal candidate for rescue and emergency operations. They are built, operated and maintained by their constituent wireless nodes. These nodes generally have a limited transmission range, so each node seeks the assistance of its neighboring nodes in forwarding packets. In order to establish routes between nodes which are farther than a single hop, specially configured routing protocols are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. Communication in mobile ad hoc networks comprises two phases, neighbor discovery and data transmission. In an adverse environment, both phases are vulnerable to a variety of attacks. First, misbehaving nodes can disrupt the route discovery by impersonating the destination, by responding with stale or corrupted routing information, or by disseminating forged control traffic. This way, attackers can obstruct the propagation of legitimate route control traffic and adversely influence the topological knowledge of benign nodes. However, misbehaving nodes can also disrupt the data transmission phase and, thus, incur significant data loss by tampering with, fraudulently redirecting, or even dropping data traffic, or injecting forged data packets.

To provide complete security in both phases of a MANET, we require secure routing protocols, since nodes involved in the routing cannot by themselves ensure the secure and undisrupted delivery of transmitted data. This is so, since misbehaving nodes could abide with the route discovery and be placed on utilized routes. But then, they could tamper with the in-transit data in an arbitrary manner and degrade network operation.

Upper layer mechanisms, such as reliable transport protocols, or mechanisms currently assumed by the MANET routing protocols, such as reliable data link or acknowledged routing, cannot cope with malicious disruptions of data transmission. In fact, the communicating nodes may be easily deceived for relatively long periods of time, thinking that the data flow is undisrupted, while no actual communication takes place.

Operation in an ad hoc network introduces new security problems. The ad hoc networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks increases [1]. Similar to fixed networks, security of the ad hoc networks is considered from the attributes such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control [2, 3]. But security approaches used for the fixed networks are not feasible due to the salient characteristics of the ad hoc networks. New threats, such as attacks raised from internal malicious nodes, are hard to defend [8]. New security mechanisms are needed to adapt the special characteristics of the ad hoc networks. In this proposed system, a novel method is proposed through which security can be provided in both phases. To enhance security in the routing phase, a trust based path routing protocol is used. It discovers a secure, trustworthy path from source to destination with minimal overhead. Misbehaving nodes are detected and exempted from such paths using the trust value of the nodes.

This paper proceeds as follows. Section 2 reports related works, highlighting existing monitoring schemes. Section 3 presents Proposed System includes TMS, emphasizing its knowledge management strategy. Section 4 presents the secured routing process algorithm using knowledge based trust. Section 5 presents the performance of proposed algorithm under PDR and End-to-End delay analysis. Finally, section 6 concludes the paper and future works.

2. Related Works

An Autonomic Trust Monitoring Scheme [1] with Secure Routing Decision Process to establish trust relations between nodes in a MANET is proposed. This work takes into account autonomic principles in order to have self-adaptive and protocol-independent trust management scheme ensures uniform distribution of trust values among nodes.

G. Bella et al. [2] presented a protocol to allow a node to evaluate the reputation of another one by means of both direct observation and recommendations received from other nodes. A Global Reputation Table (GRT), which contains the node’s view on neighbors and far nodes, is periodically exchanged with the others. Table information is not broadcasted all over the net with a flooding procedure, but when a node receives a table from one neighbor, it calculates new values, and then, with a prefixed schedule, it sends the new GRT to its neighbors. This kind of sharing limits the traffic in the net, avoiding the overload and limiting the use of energy. However, it can involve a non-uniform distribution of the same value.

Velloso et al. [3] proposed a human-based trust model, which builds a trust relationship between nodes in an ad hoc network based on previous individual experiences and on the recommendations of others. A Recommendation Exchange Protocol (REP) was proposed allowing nodes to exchange recommendations about their neighbors. The REP only considers interactions with neighbors, which makes the protocol scaling well for large networks. However, since the nodes are only aware of neighbors trust values, the detection of mobile malicious nodes can be time- consuming, especially regarding double-face attackers.

Sajal Sarkar and Raja Dutta [4] proposed a trust model which compares the mobility of the concerned nodes. They consider a point based mobility factors such as velocity, direction, and pause time. Since only mobility factors are considered to evaluate the trust factors, the detection of malicious nodes can be time-consuming and average link duration are considered for trust values.

S.Neelavathy Pari, B. Narmadhadevi and Sridaran Duraisamy [5] proposed a trust model which consider only the local trust for single hop nodes. Trust values are stored in a cluster head. Since the local trust values are evaluated for finding the routing path, the minimum number of malicious nodes will be detected. In this model, global trust is not considered.

Shusan Zhao, Robert D. Kent, Akshani aggarwal [6] proposed an integrated key management scheme for secure routing. Secure keys are available before routing starts working. Because of key exchange policy between the nodes it require some more storage and communication requirements.

Reijo Savola and Ilkka Unsitalo [7] proposed trust model which consider only the node's own responsibility. They introduced intrusion detection system for observing each node's activity. Again detection of malicious nodes was time-consuming in this method.

3. Proposed System

The proposed system consists of TMS module (Trust Monitoring Scheme), new knowledge Monitoring Scheme for trust management based on direct and indirect trust and an algorithm for secured routing process based on average trust of the nodes. The proposed system has been divided into three modules. First module is Trust Management Scheme (TMS), second is Secured Routing Decision Process, and the last module is detecting malicious nodes and secured path. Fig. 1 shows the proposed system.

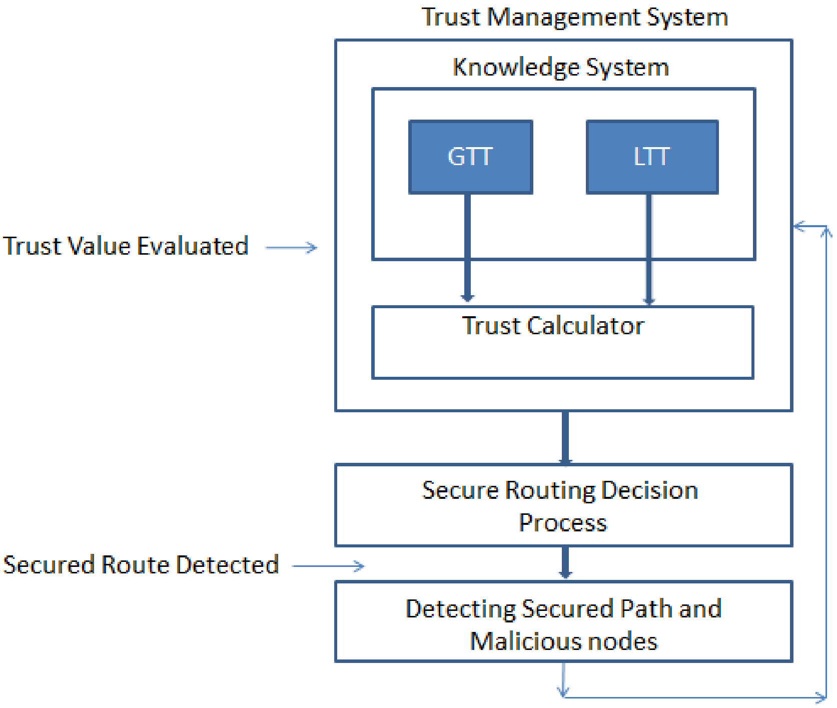

Fig1. *Proposed System Architecture*

Unlike other traditional trust strategies, the proposed trust management system employs a new technique named knowledge based trust component to help the node in better evaluating its neighboring nodes' trusts. When a node wants to evaluate a neighboring node's trust, it will send some packets to its neighboring node. Trust evaluation in routing procedure is a remark of a sender after it gets the service of a forwarding node. Packet dropping is always due to poor wireless communication quality or heavy traffic or black-hole attack or grey-hole attack. Thus we use packet forwarding ratio to evaluate the quality of forwarding.

3.1. Local Trust Derivation

The local trust monitoring module performs a local observation of neighbor nodes. a node obtains information on trustworthiness of a neighbor based on amount of traffic it receives from that neighbor.

1. When a node 'i' receives a packet from a neighbor 'j', then it checks if the packet was generated or forwarded by that neighbor 'j'.
2. The node 'i' can obtain this information just by observation of the IP header, which contains the source address of the packet.
3. A node 'i' evaluates the trustworthiness of a neighbor 'j' considering the amount of traffic it forwarded compared to the amount of traffic it generated. From the point of view of node i, this ratio represents the degree of unselfishness in the use of the link j - i.

$$R^{i}_{loc}(j) = \frac{a\,P^{i}_{f}(j) + b\,D^{i}_{f}(j)}{a\,P^{i}_{g}(j) + b\,D^{i}_{g}(j)}$$ equation (1) [2]

Where $P_x(j)$ - the packets that node j sent towards node i

$D_x(j)$ - the amount of data that they carry

The sub-index g identifies data that are generated by node j; sub-index f identifies data that node j forwards (i.e. the source is different from j). 'a and b' are different weights.

4. If amount of data generated by 'j' is > amount of data forwarded by 'j' then reputation of 'j' is low otherwise reputation of 'j' is high.
5. The basic idea is that a node reputation grows only if it forwards packets of another sender source.

The information acquired by local observation is stored in a table, called Local Trust Table (LTT). This table contains one entry by neighbor for which it stores the data amount generated and forwarded by that neighbor as well as the local trustworthiness estimated for that neighbor.

3.2. Global Trust Derivation

The global trust monitoring module is in charge of exchanging information with other nodes. Based on the table LTT, every node of the network constructs a Global Trust Table (GTT) which is gradually completed by trust values of all network nodes. To populate the GTTs with information on all participants to the MANET, nodes should exchange their GTT tables by some communication procedures. A packet can carry information on nodes, and update it continually when visiting other nodes. The global view of each intermediate node will be updated based on information carried by arriving packets. The knowledge management process decides on when it piggybacks trust information on transiting packets based on the network state. Indeed, when the network is not overloaded, the knowledge management engine activates the normal mode in which all transiting packets are used to distribute trust level information in a timely manner. For simplification, normal mode is considered for the network.

1. GTT is constructed for one-hop as well as for multi-hop nodes. Estimation of Global Reputation:

$$R^{i}_{new}(j) = w_{l}R^{i}_{loc}(j) + w_{r}(w_{2}R^{i}_{est}(j) + w_{3}R_{rec}(j))$$ equation(2) [2]

Where $w_l + w_r = 1$ and $w_2 + w_3 = 1$ (adequate weights)

$R^{i}_{est}(j)$ – estimated trust value of node 'i' on 'j' and stored in GTT

$R_{rec}(j)$ – recommendation about 'j' received from other neighbors

2. This reputation value is stored in GTT.
3. GTT is gradually completed by trust values of network nodes.
4. GTT populated to all participants on the network.

3.2.1. Finding Average Trust for all the nodes

Step1. All nodes are initialized to minimum trust value 0.1.

Step2. Finding the neighbors and Trust calculation starts from 0th node.(central node)

Step3. The central node starts listening to the neighboring nodes to calculate the trust values.

Step4. After calculating trust values, the highest trusted node in that will be the trust agents which act as assistants to the central node and fulfill the role of helping the central node to calculate the trusts of other nodes. When the central node wants to evaluate a neighboring node's trust, it will query its trust assistants about this neighboring node.

Step5. If trust value < 0.5 then node = untrusted

else trust value > 0.5 node = trust

Step6. Calculated trust values are stored in a trust table GTT.tr.

Step7. Step 1 has been repeated for all the nodes in the network.

4. Secure Routing Process

In this section, an algorithm for secure routing decision process based on knowledge based trust values of the node is detailed below. Source node broadcasts routing request message to its neighbors in order to find a route to destination node. It has been shown in Fig. 2.

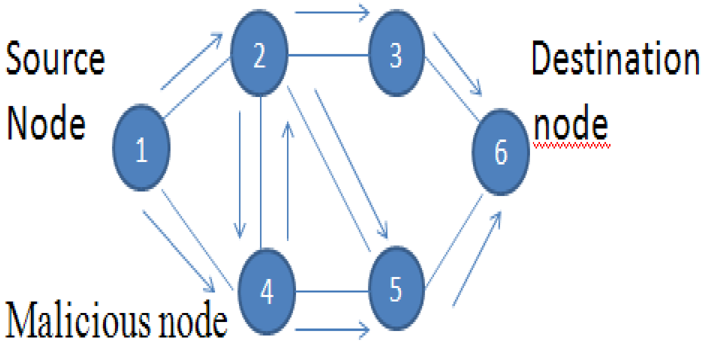

Fig3. *Routing Request*

The neighbors of the source node forward the request to their neighbors if the trust evaluation on the source node passes its predefined threshold, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached. And that node would like to accept the data transfer based on its trust evaluation. If some nodes respond that they have fresh enough route to the destination node and would like to reserve some time slot for serving data transfer, the source node checks the trust evaluation using TM System on the responded nodes. Based on the trust evaluation result and hops of the routes, the source node selects one preferred route, which it believes the best. It has been shown in Fig. 3.

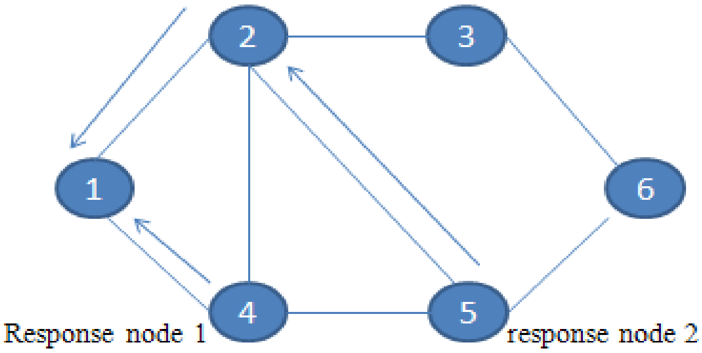

Fig4. *Routing Response*

After receiving the data packages, the destination node applies the same method above to reply the confirmation message if the source node requests it.

4.1. Path's Trust Computation

A novel method is proposed to enhance security in mobile network. A secured routing protocol is designed based on trust, which ensures secure and undisrupted delivery of transmitted data. The misbehavior mentioned above can be nullified by securing the data transmitted. We have assumed that each node creates a Trust Table and stores the trust value of its one-hop neighbors. The trust value is assigned in the range from 0 to 1. A well behaved node is assigned trust value >= 0.5, while a malicious node is assigned trust value < 0.5 and particularly trust value < 0.2 is attacker. The trust value of a node is computed and updated by trust agents that reside on network nodes. We do not consider physical layer and link layer attacks, like jamming attacks, in this project. We introduce the concept of path trust which is derived from the mutual trust value of nodes involved in the path and the total number of nodes. Furthermore, malicious nodes can be avoided from the path as the most trustworthy path is selected.

Path trust is the trust value associated with the path. This value is defined as the weighted average of the trust values of the nodes in the path. Trust is considered to be asymmetric, so mutual trust between the nodes is used. Hop count also plays a prominent role in the selection of the path since the larger the number of nodes, more is the delay in the network and chances of information modification also increases. To calculate path trust, the neighbor discovery packets are modified so that they contain the trust value of the node from which the packet is received. Both packets are changed because during route discovery a node transmits the topology discovery packet by broadcasting. A node knows only the node from which the packet is received, not the node to which it is to be transmitted. Therefore, the topology discovery packet is modified to incorporate the previous node's trust value. For example, if there are two nodes A and B in the network, when B broadcasts a topology discovery packet and node A receives it, it updates the P_TRUST field as:

$$P\_TRUST = P\_TRUST+T(AB)$$

Where T(AB) is the trust value that is assigned by node A to B and signifies how much node A trusts B. When the topology discovery packet reaches the source node, it calculates path_ trust which is the trust value associated with the path. Path_trust is a weighted average based on the trust values p_trust and n_trust received in the topology discovery packet and the number of nodes in the path as shown in below.

Trust value of the path is

$$P\_trust = p\_trust + n\_trust$$

$$\text{Path trust (s-d)} = \max (p\_trust)$$

Where n is the total number of nodes in the path.

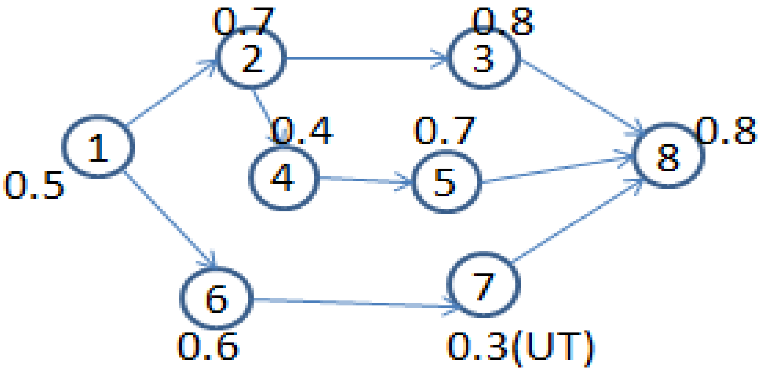

Fig5. *Path Trust Computation*

As shown in Fig.5, node 1 is source node and node 8 is the destination node. Source node sends RREQ to its neighbors along with its trust values. The neighbor node which is having fresh enough route to the destination sends RREP to the source node along with their trust values. Source node then, checks the route for untrusted node exists in the route. If untrusted exist, then that route is discarded by the source node and calculate the path trust for the rest of the routes. Path trust is initialized to 1. Two paths are there from source to destination.

One is 1 →2 → 3 → 8 having path trust as 28 and Second path is 1 → 2→ 4 → 5 → 8 having path trust 24. In this, Path trust(S – D) = MAX(path-trust) will be selected, so the first path is selected as its' path trust is 28.

5. Performance and Results

We have implemented the proposed system using NS2 simulation tool. Two metrics are related to network in our evaluations. As network performance metrics, we have the Packet Delivery Ratio (PDR) and the Average E2E delay.

The former consists in the number of data packets successfully delivered at the destination divided by the number of data packets sent from the source. The latter lies in transmission delay of data packets delivered successfully, consisting of propagation delays, queuing delays at interfaces, retransmissions delays at the MAC layer, as well as buffering delays during the route discovery.

The Distributed Coordination Function (DCF) of IEEE 802.11[29] for wireless LANs is used as the MAC layer protocol. 50 nodes are randomly dispersed in a rectangular field with 1000m×1000m. The transmission radius of every node in one hop is fixed at 250m. The node mobility uses the random waypoint model in which each packet starts its journey from a random location to a random destination with a randomly chosen speed.

Table1. *Experimental Setup*

Protocols	AODV
Simulation Time	500 seconds
Number of Nodes	50
Map size	1000mx1000m
Mobility	Random way point
Traffic Type	Constant Bit Rate/UDP
Transmission Radius	250m
Packet size	512 bytes
Connection Rate	4pkts/sec

The trust threshold η is set to 0.5, which means the node with trust value less than 0.5 will be regarded as a malicious node and added into the black list. The length of the time window w in formula (1) is set to 500 seconds. That is, packet forwarding ratio is computed by the cumulative count of correct forwarding and the total count of all requesting from the beginning (t=0).

In the below fig. 6, 7, 8, 9, 10 and 11, performance of existing and proposed system is shown on the basis of PDR, End-to-End Delay, and packet Drop metrics for the number of nodes 20 and 50. The proposed system is having the high PDR, less End-to-End delay, and reduced packet drop than the existing system. Green line is for existing system and red line for proposed system.

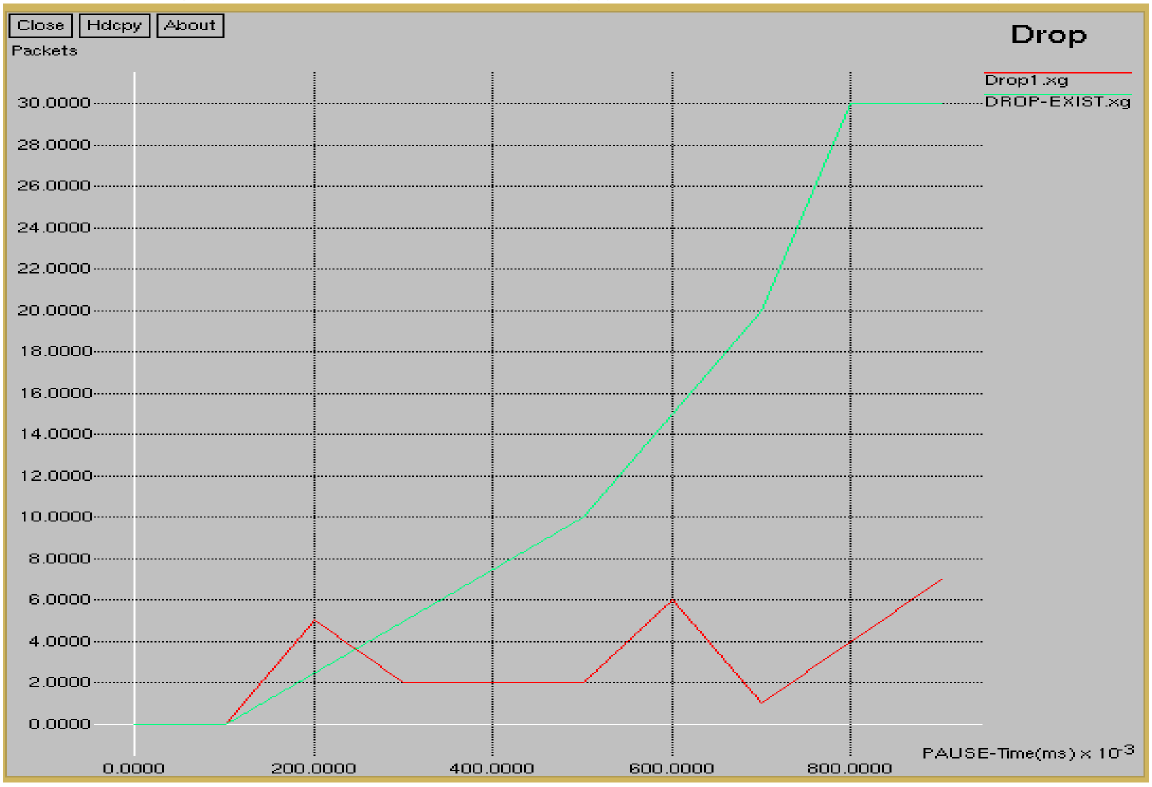

Fig6. *Packet Drop for Number of nodes 20*

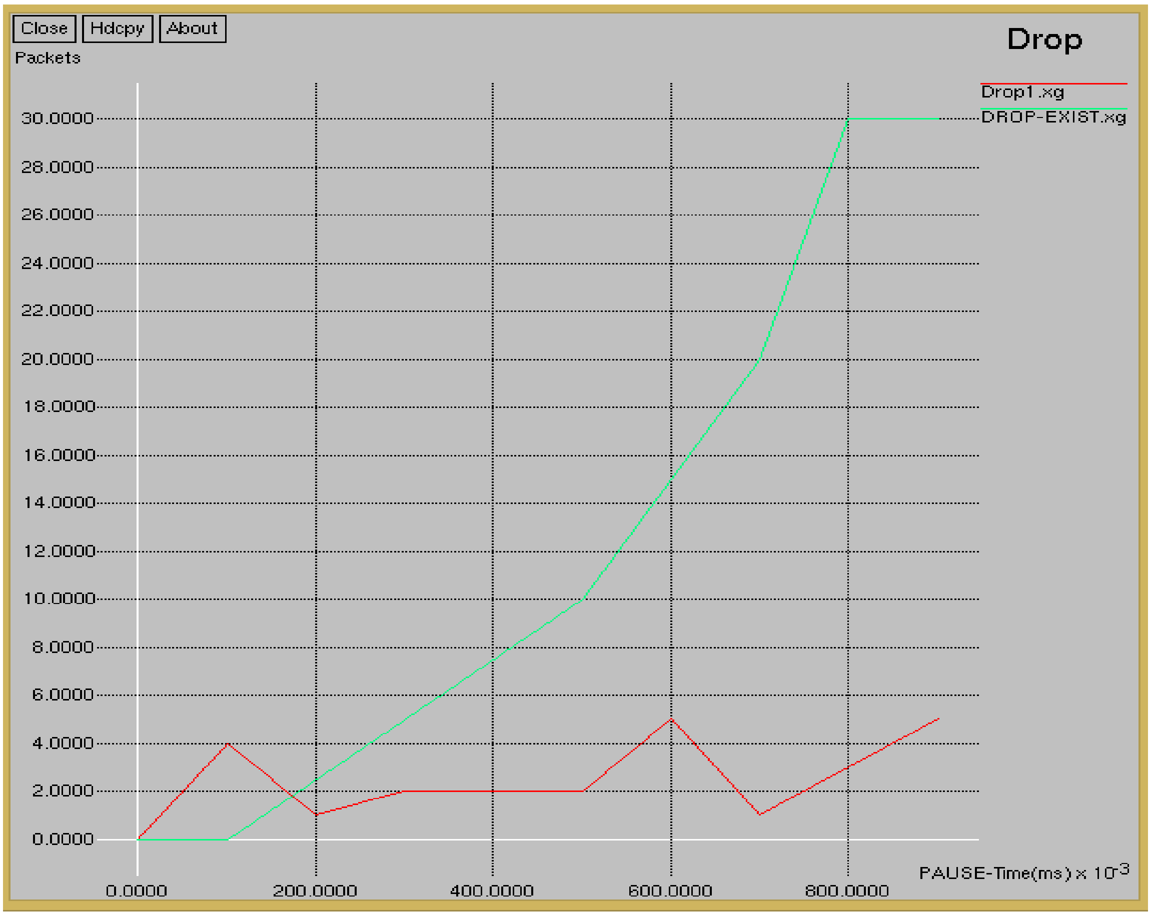

Fig7. *Packet Drop for Number of nodes 20*

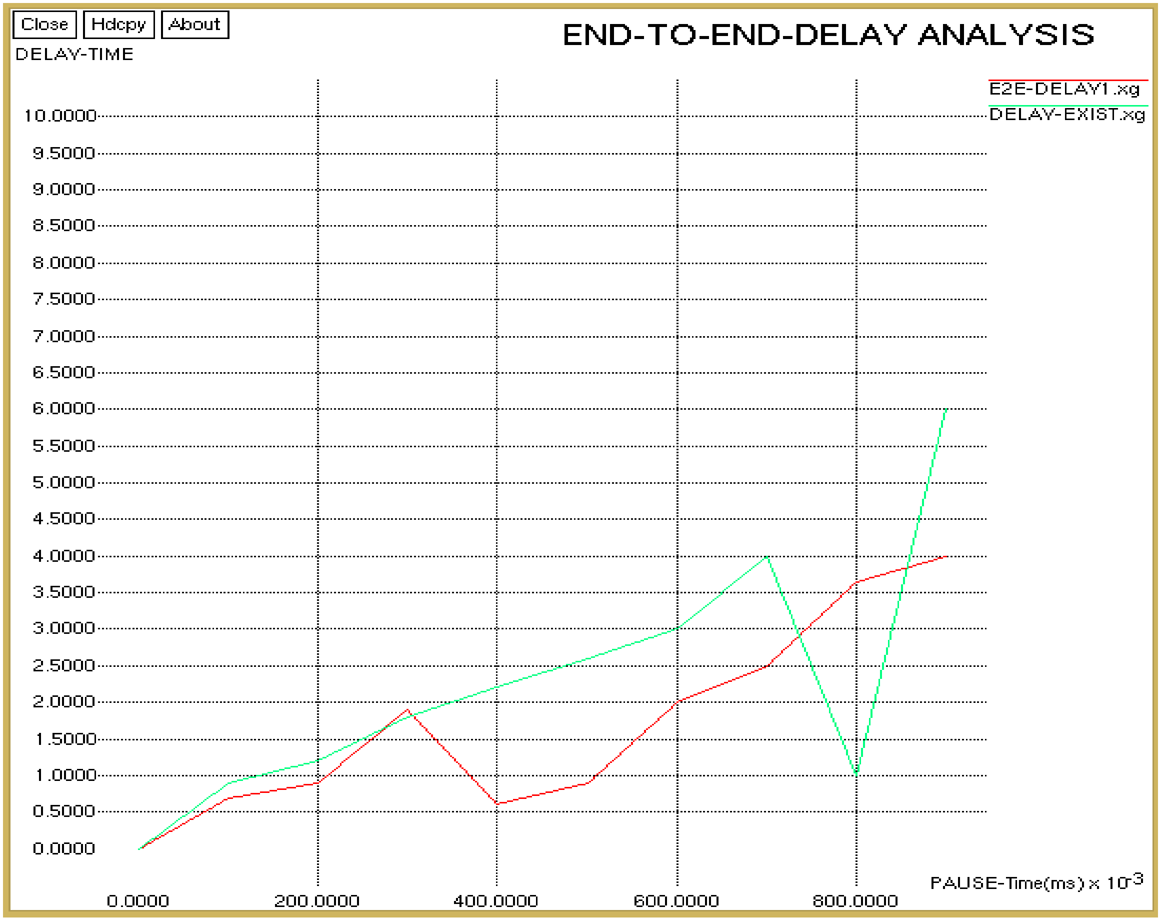

Fig8. *E2E Delay for number of nodes 20*

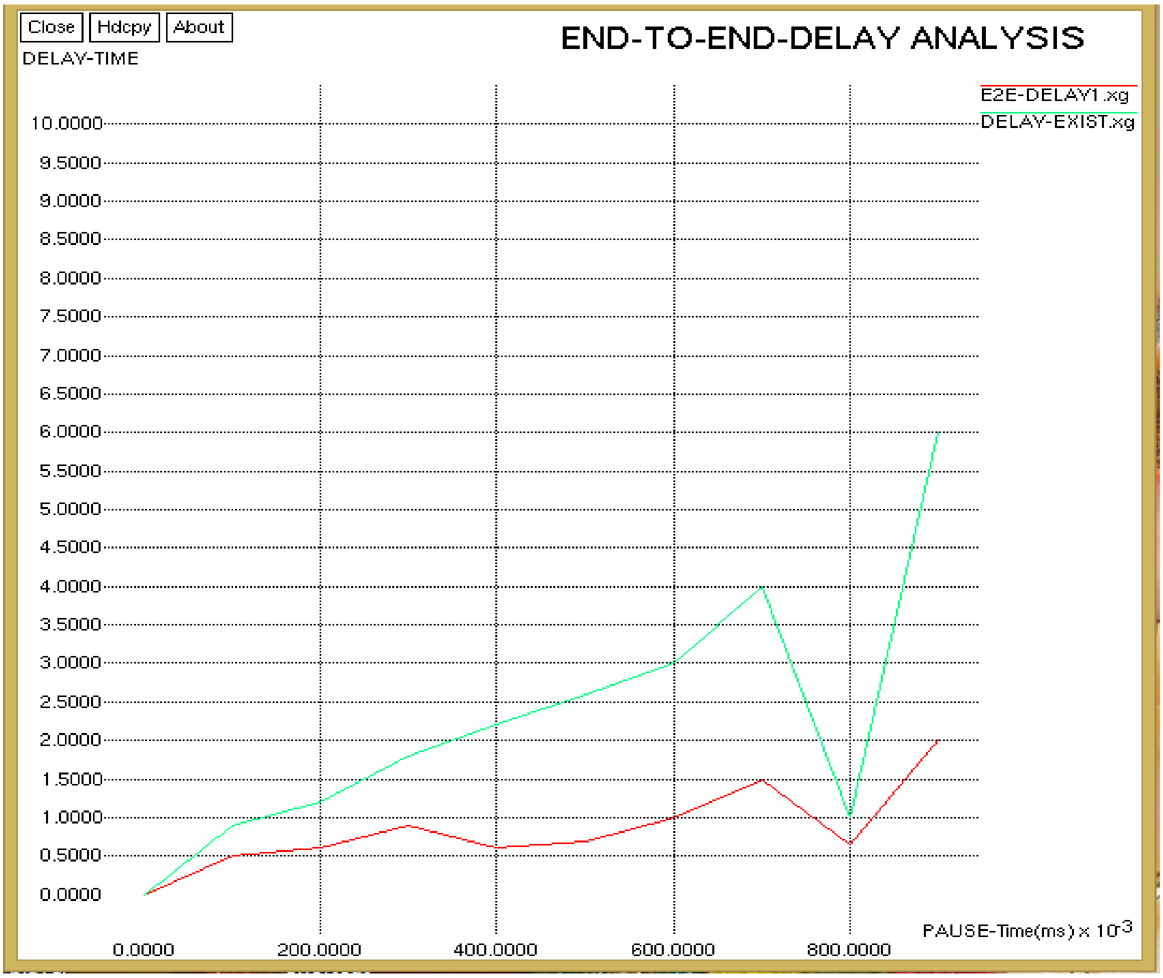

Fig9. *E2E Delay for number of nodes 50*

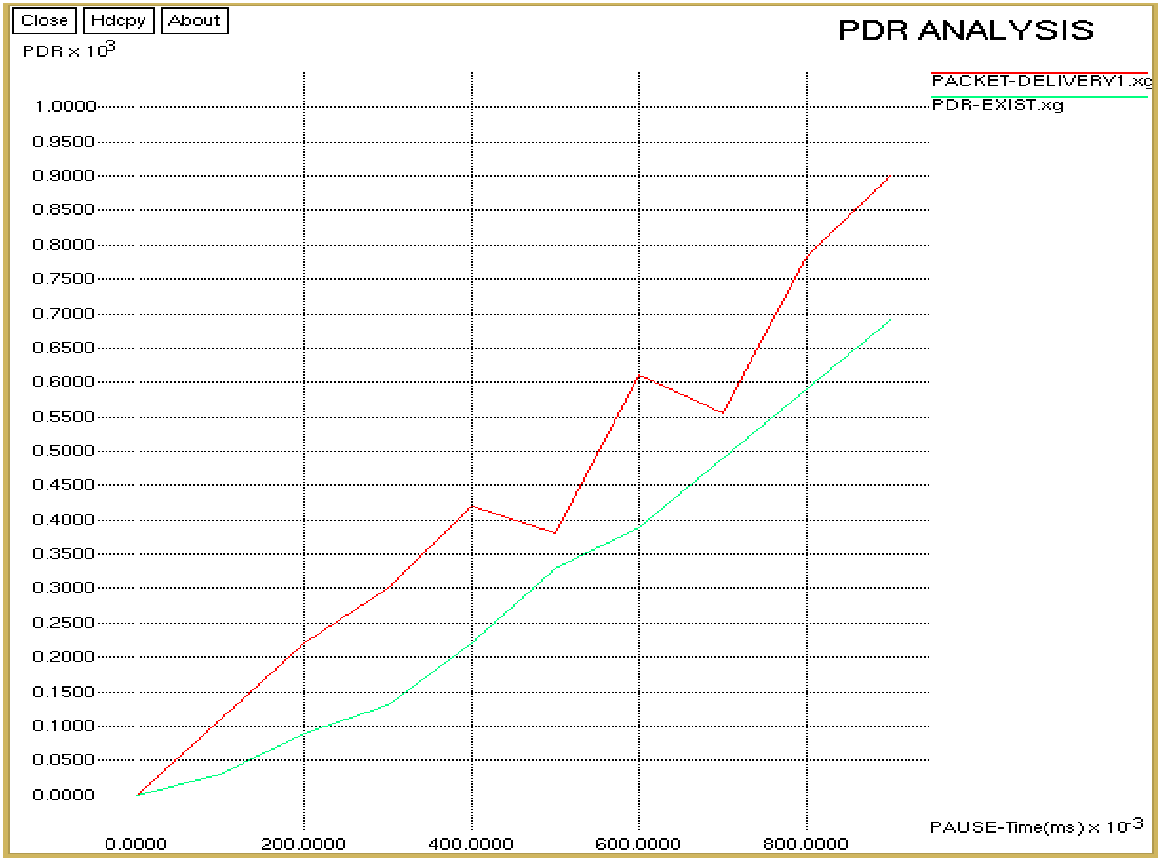

Fig10. *PDR for number of nodes 20*

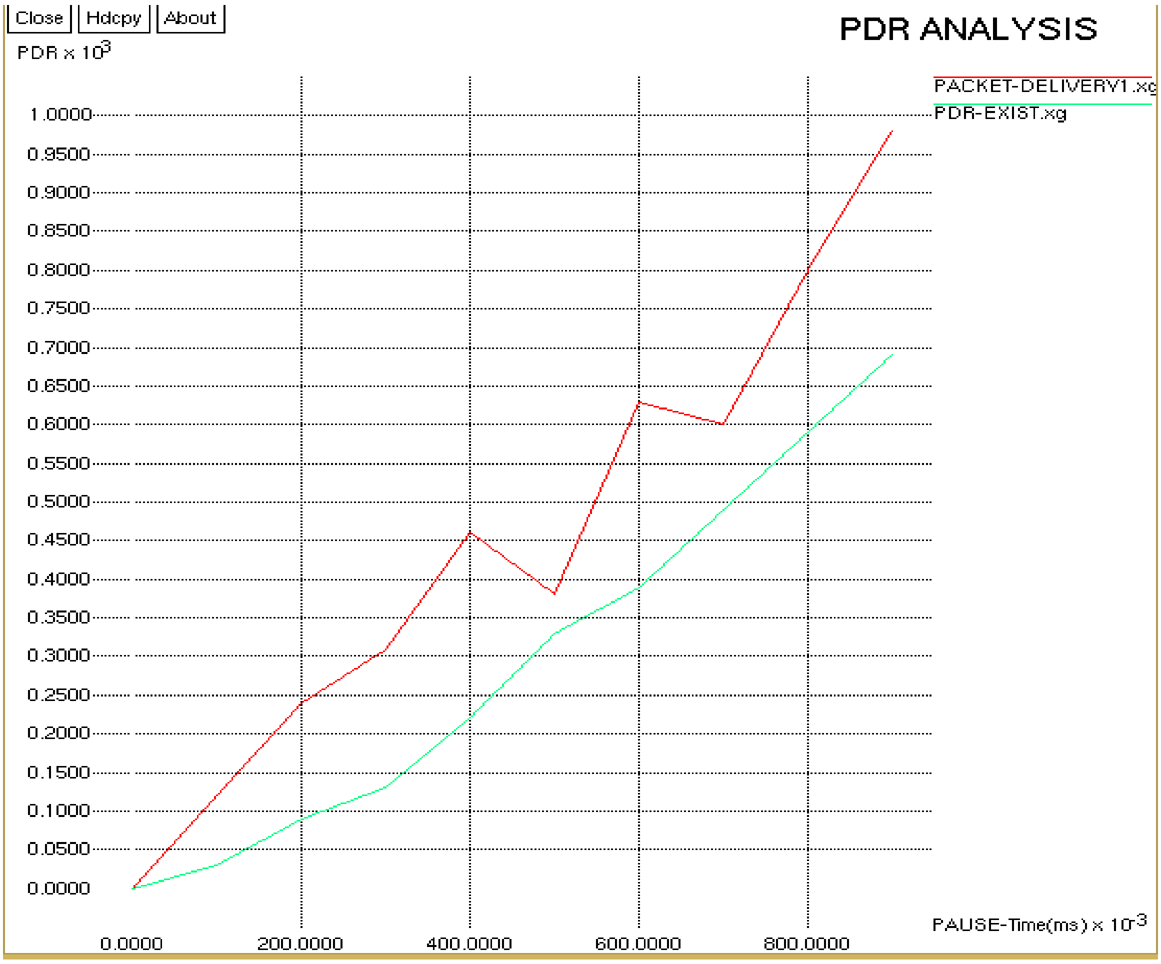

Fig11. *PDR for number of nodes 20*

Table2. *Analysis for 50 nodes*

	Drop (10^3)		**PDR (10^3)**		**End-to-End Delay**	
	Pause Time	**Packet Drop**	**Pause Time**	**PDR values 10^3**	**Pause Time**	**Delay Time**
Existing system 50 nodes			0.0		0.0	
	0.1	0.0	0.1	0.3	0.1	0.9
	0.5	0.1	0.2	0.9	0.2	1.2
	0.7	0.2	0.3	0.13	0.3	1.8
	0.8	0.3	0.4	0.12	0.4	2.2
	0.9	0.3	0.5	0.33	0.5	2.6
			0.6	0.39	0.6	3
			0.7	0.49	0.7	4
			0.8	0.58	0.8	1
			0.9	0.69	0.9	6
Proposed system – 50 nodes	0.0		0.0		0.0	
	0.1	0.4	0.1	0.12	0.1	0.5
	0.2	0.1	0.2	0.14	0.2	0.6
	0.3	0.2	0.3	0.31	0.3	0.9
	0.4	0.2	0.4	0.46	0.4	0.6
	0.5	0.2	0.5	0.38	0.5	0.7
	0.6	0.5	0.6	0.63	0.6	1
	0.7	0.1	0.7	0.60	0.7	1.5
	0.8	0.1	0.8	0.80	0.8	1.6
	0.9	0.5	0.9	0.98	0.9	2

In the above analysis, has been taken for 50 nodes, End-to-End delay is decreased to some extent than the existing system. Packet drop is decreased in the proposed system and PDR is improved better than the existing system. In the above table, analysis is shown for 50 nodes only but the graph has been drawn for 20 and 50 nodes. In that the End-to-End delay is increased for 20 nodes in proposed system because in the sparse network if untrusted nodes are more then, it is difficult to find out the route so E2E delay is increased. The same analysis has been done for 20, 40 and 80 nodes in a network, we observed that end-to-end delay is increased for sparse network and it is decreased for dense network say 50 and above.

6. Conclusion

This work is described a knowledge trust monitoring scheme and a secured routing decision scheme for MANETs. Its main goal is to provide trust knowledge throughout the network with a minimum monitoring overhead and detect the denial of service attack. This knowledge based trust secured routing protocol is characterized by its protocol and trust framework independence, self-adaptation, simplicity and low computational intensiveness. . In the above table, analysis is shown for 50 nodes only but the graph has been drawn for 20 and 50 nodes. In that the End-to-End delay is increased for 20 nodes in proposed system because in the sparse network if untrusted nodes are more then, it is difficult to find out the route so E2E delay is increased. Our proposed system works very well for dense networks.

This can be extended to find multiple paths and from that multiple paths highly trusted shortest path can be selected. Further it can be extended to include multiple hops to find out the secure routing.

References

[1] Z.Movahedi, M.Nogueria and G.Pujolle, An Autonomic Knowledge Montoring Scheme for Trust Management on Mobile Ad hoc Networks IEEE wireless communication and Networking Conference, 2012.

[2] G. Bella, G. Costantino, and S. Riccobene, Managing reputation over MANETs. In Proceedings of the Fourth International Conference of Information Assurance and Security, pages 255–260, Washington, DC,USA, 2008.

[3] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, Trust Management in mobile ad hoc networks using a scalable maturity Based model. IEEE Transactions on Network and Service Management,7(3):172–185, 2010.

[4] Sajal Sarkar and Raja Dutta, A Mobility factor based Path Selection for Mobile Ad-hoc Networks, IEEE, 2012.

[5] S.Neelavathy Pari, B. Narmadhadevi and Sridaran Duraisamy, Requisite trust-based Secure routing Protocol for MANETs, ICRTIT, IEEE, 2012.

[6] Shusan Zhao, Robert D. Kent, Akshani aggarwal, An Integrated Key Management and Secure Routing Framework for Mobile Ad-hoc Networks, Tenth Annual Conference on Privacy, Security and Trust, IEEE, 2012.

[7] Reijo Savola and Ilkka Unsitalo, Towards Node-Level Security Management in Self-Organising Mobile ad-hoc Networks, IEEE,2006.

[8] S. Corson, J. Macker, Mobile Adhoc Networking (MANET): Routing Protocol Performance Issue and Evaluation Considerations, IETF RFC2501, 1999.

[9] L. Zhou, Z. J. Haas, securing Adhoc Netowrks, IEEE Networks, 13(6): 24-30, Nov/Dec 1999.

[10] Y. Zhang, W. Lee, Intrusion detection in Wireless Ad hoc Network Proceedings of mobicom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11, Aug 2000.

[11] H. Deng, Wei Li, A. P. Dharma, Routing security in Wireless Ad Hoc Networks, IEEE Communications Magazine, p70-75, Oct 2002.

[12] J. Hu and M. Burmester. Cooperation in mobile ad hoc networks. In Guide to Wireless Ad Hoc Networks, Computer Communications and Networks, pages 43–57. Springer London, 2009.

AUTHORS' BIOGRAPHY

K.S.Charumathi has completed Bachelor's Degree from Bharathidasan University, Tamil Nadu, and doing Master's Degree at Pillai Institute of Information Technology, Mumbai University, Mumbai. She is having more than 8 years of experience in teaching field. Her area of interest is in Networking and Security. Her Master's thesis is focused on Security in mobile ad-hoc networks, doing under Dr. Madhumita Chattejee who has completed her P.hd degree from IIT , Mumbai.

Dr. Madhumita Chatterjee has completed her P.hd from IIT, Mumbai. She is now working as HOD of Computer Engineering Department at Pillai Institute of Information Technology, Navi Mumbai, Maharashtra. She is having teaching experience over 20 years and providing her valuable guidance to her students in many research areas like network security and cyber security. She has conducted many workshops on Network Security and worked as a coordinator for many workshop, conducted by IIT, Mumbai.