MANET Security for Reactive Routing Protocol with Node Reputation Scheme

[1]A. Suresh and [2]K. Duraiswamy
[1]Department of MCA, [2]Department of CSE,
K.S.Rangasamy College of Technology,
Tiruchengode.637 215, Tamil Nadu, India
[1]asuresh1975@yahoo.com; [2]drkduraiswamy@yahoo.com.

Abstract

The mobile node's reputation in the Mobile Ad hoc Network (MANET) identifies its trust worthiness for secured multiple data communication. Unknown nature of the node's communication status for initial period has great impact in the effective data transfer as MANET is self-organized and distributed. The functional operation of the mobile network relies on the trusty cooperation between the nodes. The major factor in securing the MANET is based on the quantification of node's reputation and trustworthiness. The previous literatures provided uncertainty model to reflect a node's confidence in sufficiency of its past experience, and effect of collecting trust information from the unknown node status. With node mobility characteristic, it reduces unknown nature and speed up trust convergence. Mobility-assisted uncertainty reduction schemes comprised of, proactive schemes, that achieve trust convergence and reactive schemes provide node authentication and their reputation. They provide an acceptable trade-off between delay, and uncertainty. The mobility based node reputation scheme presented in this paper, identifies and monitor the node's trustworthiness in sharing the information within the ad hoc network. Mobile nodes information uncertainty is handled with the mobility characteristics and its reputation is evaluated to trust or discard the node's communication. Simulations are carried out to evaluate the performance of mobility based node reputation scheme by measuring the nodes consistency behavior, neighboring communication rate, and path diversity. The average node's neighboring communication rate is high for the proposed mobility based reputation scheme compared to the reactive routing protocols.

Keywords: MANET Security, Reputation scheme, Mobility, Trust

1. Introduction

A MANET can be considered as the collection of wireless mobile nodes organized to create a temporary connection between them. Neither pre-defined network infrastructure nor centralized network administration exists to assist in the communication in MANETs. Through a direct shared wireless radio links nodes communicate with each other. Each mobile node has a limited transmission range. Using a multi-hop strategy nodes wishes to communicate with other nodes outside their transmission range. There are two types of MANETs: closed and open [1]. In a closed MANET, all mobile nodes cooperate with each other toward a common goal. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity.

As the node participates in the network functions some resources are consumed quickly. For instance, battery power is considered to be most important in a mobile environment. At any cases an individual mobile node refuses to share its own resources. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Those nodes are termed as selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior [2]. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission [3]. In order to conserve its own energy a selfish node may refuse to forward data broadcasting has been used. The solution is not vulnerable to this behavior. In this method, each node broadcasts a RREQ packet if it is received from different neighbors. Therefore at the destination have multiple reputation count value for different nodes, which further lead to the discovery of the most secure path, avoiding misbehaving nodes.

packets for other nodes. The proposed solution finds a secure, trustworthy path from source to destination. Such a path is free from any misbehaving nodes. Take into consideration both the trust value of the nodes in the path and also the number of hops involved to search for a path from source to destination

In the traditional DSR protocol [10] when a desire node receives a RREQ packet, it checks if it has previously processed it or not. If it has processed it drops the packet. A misbehaving node takes advantage of this and forwards the RREQ fast so that the RREQ from other nodes are dropped and the path discovered includes itself. In this proposed work a different approach for RREQ packet

2. Related Work

Much research work has been done to make the route discovered by Mobility based Node Reputation Scheme (MNRS) secure. Various frameworks [3] have been designed to model trust networks and have been used as trust management systems [4]. It can be divided into three

main categories. In the first category the trust management system has a central authority, which is usually called the Trusted Third Party (TTP). Entities cooperate on the basis of the trust values (e.g., the authorization certificates) assigned by the TTP. Introducing a TTP will violate the self-organized nature of MANETs, which makes these systems inapplicable in MANETs.

In the second category, one global trust value is drawn and published for each node, based on other nodes' opinions toward it. EigenTrust [1] is one mechanism in this category. The algorithm calculates the computation of global trust values in the distributed environment. EigenTrust presents the request to separate misbehavers from newcomers. But, it lacks the method to satisfy this request naturally. EigenTrust is a representative and most existing trust evaluation systems have the same requirement, but omit uncertainty at the same time.
In the third category, it includes the trust management systems that allow each node to have its own view of other nodes. These systems are more realistic as they are similar to the trust models in the social network. Each node builds its view based on the observation as well as the recommendation from others. Many recent reputation systems, such as CONFIDANT [2], CORE [5], and OCEAN [6], belong to this category. In the improved CONFIDANT [7], Buchegger and Boudec provided a modified Bayesian approach for reputation representation, updates, and view integration. When updating the reputation according to recommendations, only information that is compatible with the current reputation rating is accepted. This approach is objective and robust. But, this approach still leaves an opportunity for elaborate attackers to launch false accusation attacks since there is no constraint on update frequency. This approach also lacks the ability to separate newcomers from misbehavers.

A Trust based routing is proposed by Pirzada [8] in which the trust agent derives trust levels from events that are directly experienced by a node. Trust information is shared by the Reputation agent about nodes with other nodes in the network. A Combiner computes the final trust in a node based upon the information it receives from the Trust and Reputation agents. Trust is computed using direct and indirect information. The trust value is propagated by piggybacking the direct trust value of the nodes along with RREQ packets [8]. Each time a packet is forwarded or sent, the routing table is being scanned for all alternate paths leading to the destination. It compares the direct trust value of all next hops in this path and selects the one with the highest trust value.

Routing Algorithm based on trust was also proposed by Wang et al [11]. In advance the trust values of all the nodes are assumed and are stored at each node. Trust for the route is calculated at the source node based on the weight and trust values are assigned to the nodes involved in the path at the source node. Assignment of weights is done ranging from 0 to 1. The protocol uses the path with the largest trust value of route and least packet delay from among multiple route options, as metrics, unlike the standard DSR protocol that only uses minimum hop count. In [12], [13], Wu and coauthors raised the question of whether mobility should be treated as a foe (undesirable) or a friend (desirable). In security-related research, this question also attracted a significant amount of research interest [14].

A formal trust structure was proposed [8]. In order to reflect the uncertainty the trust structure allows for an interval between belief and disbelief. The narrower the interval, the lower the uncertainty. The trust domain so obtained in [8] was particularly interesting, interesting from the findings, as it allows for the expression of complex policies. However, the focus of the trust structure is not the specific definition of uncertainty. The notion of uncertainty can also be integrated into formally defined trust structures and adopted in enriched policies. Josang [9], developed algebra for assessing trust relations, and it has been applied to set up certification chains. A triplet designating belief, disbelief, and uncertainty is assigned to each trust statement.

3. Mobility Based Node's Reputation Scheme

Mobility pattern of most nodes in MANETs is determined by their own tasks and considered to be random; the controlled-movement-based schemes in MANETs usually assign the specific task to a selected small portion of nodes to enhance the performance. Unknown status of the mobile node is the main element in trust evaluation. In MANETs, mobility increases the chance that two separated nodes meet and directly contact each other. It also allows each node to have more evidence to verify future recommendation.

In the proposed mobility based node's reputation scheme, each node has one unique ID and it cannot be spoofed. A node can only monitor the behavior of its 1 hop neighbor. When two nodes directly contact each other in 1 hop, they have a way to decide whether the result is satisfactory, nodes' behaviors are consistent. A node's general behavior can be deduced from its past actions; nodes are independent from each other, with no collusion. The proposed reputation system accommodate independent false positive and false negative. The knowledge of reputation reflects the focus of a trust evaluation system. Reputation is the opinion of one entity toward another based on past experiences. In most of the existing systems, reputation is represented as two variables: belief and disbelief. However, dividing trust into only belief or disbelief is not always appropriate. One reputation value based on 10 contact experiences, and another based on 100 contact experiences, have totally different meanings. An ordering between no knowledge and total certainty is needed to reflect the degree of confidence in trust information.
In this system, a one-dimensional representation of belief, disbelief, and uncertainty is extended from the subjective

logic. Each node keeps a belief and disbelief value toward other nodes as a prediction of their future behavior. As these two values are only predictions, uncertainty always exists. The node's opinion is represented as designated as belief, disbelief, and uncertainty, respectively. The reputation of a node computed from first-hand information is the reputation based on one's own experience. It is calculated directly from a node's observation. Each node will also propagate this information so that other nodes can use it as second-hand information. Each node estimates its neighbor's reliability based on its accumulated observations using Bayesian inference.

Bayesian inference is a statistical inference in which evidence or observations are used to update or to newly infer the probability that a hypothesis may be true. Beta distributions, Beta are used here in the Bayesian inference, since it only needs two parameters that are continuously updated, as observations are made. To start, each node in the network has the prior Beta for all its neighbors. The prior Beta implies that the distribution of the reliability metric complies with the uniform distribution, which indicates complete uncertainty as there are no observations. When a new observation is made, if it is a successful forwarding, then it is updated. The prior is then updated as Beta when needed. The triplet representing the node's opinion is derived from Beta Reputation exclusively based on direct contact increases the detection time when compared to an approach that also uses reports from others. The more information each node considers, the faster the trust evaluation achieves convergence. Second-hand information is the information that a node gets from the first-hand information published by other nodes. It is a kind of trust transitivity. Node A first gathers other nodes' first hand observations toward node C. Node A converts the information into an opinion and discounts it by node A's opinion toward the node reporting the observation. The recommendation is calculated in this sense. After gathering all the recommendations, node A will synthesize them and integrate the second-hand information with the first-hand observation and make a final anticipation and decision.

The reactive routing model in which dropping of the subsequent RREQ packet may lead to following problems:

a. In the traditional reactive protocol when a node receives a RREQ packet, it checks if it has previously processed it or not. If it has processed it drops the packet. An adversary node takes advantage of this and forwards the RREQ fast so that the RREQ from other nodes are dropped and the path discovered includes itself.

b. Compared to the paths with congested or high areas of mobile network RREQ packets arrive quickly compared to the paths with congested or highly mobile areas of the network. This results with no path through congested or highly mobile area. But if there exists a shorter path and if such areas are recovered quickly then such shorter path may not be utilized.

c. One of the other drawbacks is that all the one hop neighbors of destination after receiving first RREQ propagate to destination. This results in discarding the RREQ packet from most of the neighboring paths.

To take into consideration the above problems, the following modification is proposed to the traditional reactive routing protocol and present efficient MNRS. MNRS discovers multiple neighbor reputation between two nodes. This is essential for an ad hoc network to be able to tolerate attack-induced path failures and provide robust packet delivery. Depending on the number of nodes in the ad hoc network the node's reputation count status is used. If robustness is required, it can send the same packet through those trusted neighbor so high reputation. Each node creates a Reputation Counter Table as shown in Table 1. This table maintains a reputation count value for its node neighbors. In the proposed work, each node stores the reputation count value of its node neighbors.

Table 1. Reputation Counter Table for Node Neighbors

Node Neighbor	Reputation counts
B	0.74
C	0.83

The reputation count value is assigned in the range from 0 to 1. A well behaved node is assigned reputation count value >= 0.5, while a malicious node is assigned reputation count value < 0.5. Do not consider physical layer and link layer attacks, like jamming attacks, in this paper. To decrease the routing overhead and increase the network performance all the one hop neighbors of destination unicast the RREQ packet. In reactive routing protocol there is no procedure to know the one hop neighbors of destination as no next hop table is maintained. Therefore to address the above problem we maintain neighbor table as shown in Table 2 at every node in MANETs. This table is used to maintain all the neighbor hop nodes to its respective destination. It has two fields which are destination node in which it stores the name of the node i.e., assigned name to whom the RREQ packet is designated and the other field is neighbor hop nodes which store the total hop neighbor nodes of appropriate destination. This table is created when a new RREQ packet is received at each intermediate node.

Table 2. Neighbor Table

Destination Node	Neighbor Hop Nodes
E	18
F	16

3.1 Routing Node Discovery

If a path is already not known and supposes a source node wants to transmit a data packet to a destination node, it first initiates a route discovery process by broadcasting a route request packet. The RREQ packet header is modified by adding a p_truste field, so that it now contains the following fields: source IP address, destination IP address, a sequence number and p_truste:

RREQ:
{IPsource, IPdes, Seq num}|| p_truste (1)

where IPsource and IPdes are IP addresses of the destination and source nodes, Seq num is the sequence number .

It is maintained by the source node for each destination node and increases automatically for each route request. p_truste denotes the trust value of the path up to that node and is initialized as 0 at source node.
After broadcasting the RREQ packet, the source node sets a timer whose time period T which is equal to 1-way propagation delay. It is determined by using formula given below:

$$T = 2 * MAX_{TR} / Sp + n \quad (2)$$

where MAX_{TR} = maximum transmission range.

Sp = Speed of the wireless signal.
n = Neighbor node rate threshold constant, TR/2*S as used in simulation.

The time value of the timer set to denote the time needed to receive a RREP packet from one hop neighbors. Based on the arrival time and the length of the path, the acceptance of RREP is denoted. The possible arrivals for RREP packet could be before or after the timer expires. Accordingly either it can be accepted or rejected. If RREP packet arrives before the timer expires then it is accepted if path length is equal to 1 else it is rejected. As this RREP packet may be forged RREP packet form a malicious node. If path length is greater than 1 it arrives after timer expires and the value is greater than 1. As now the RREP packet has traversed along the path containing only legitimate nodes from source to destination. RREP packet is rejected if path length is 1 as it is from malicious node.

3.2 Processing of route request at intermediate nodes

Processing takes place only when the packet is received from a different path. When an intermediate node receives the RREQ packet, it is processed and sees to that it is not from the one hop neighbors of destination and does not include one hop neighbor of destination. So there is a propagation delay which is being done by the intermediate node. The time delay to forward RREQ by is equal to 1-way propagation delay. The above said process is performed only after receiving the RREQ packet. The delay D_{fac} is calculated using formula given below.

$$D_{fac} = MAX_{TR} / Sp + n \quad (3)$$

where MAX_{TR} = maximum transmission range.
n = constant value, TR/2*S as used in simulation.

If the intermediate node overhears a RREP packet with hop count equal to 1 before the timer expires, then intermediate node and the node that forwarded the RREQ packet are both one hop neighbor of destination. So the neighborhood table is updated by storing intermediate and forwarding node as one hop neighbor of the specified destination. If the intermediate node is one hop of destination The RREQ is forwarded in unicast manner it is broadcasted. This ensures lesser routing overhead as unicast the RREQ packet by such intermediate node decrease routing packets in the network.

Unlike previous approaches which are based on broadcast and hence ignore the path from one hop neighbor of destination, the protocol proposed in this paper consider such path as it uses unicasting of route discovery packet from one hop neighbor of destination which lead to detect most trustworthy path. So the increase in detection rate of misbehaving node lowers the packet drop attack which indirectly increases throughput of the network. Each RREQ packet is modified to include the trust value of the node from which packet is received. So when B broadcasts a RREQ packet and node A receives it, it updates the p_truste field as:

$$p\_truste = p\_truste + trust_{AB} \quad (4)$$

where $trust_{AB}$ is trust value that is assigned by node A to B and signifies how much node A trusts B.

3.3 Destination node's route of reply

When a destination node receives RREQ it immediately sends RREP. At the destination, p_truste contains information about the trust of all nodes involved in the path.

The RREP packet header is modified such that it contains two fields p_truste and n_trust in addition to other fields. The updated RREP PACKET is:
RREP :
{IPsource, IPdes, Seq num}|| p_truste|| n_trust (5)

Where p_truste is assigned from the RREQ packet received at the destination and n_trust is initialized to 0. It has the same significance as p_truste in the RREQ packet

and denotes the trust value of the path up to that node from the destination.

3.4 Processing of intermediate nodes at RREP

When an intermediate node receives a RREP PACKET, it checks if it is the intended next recipient. If yes, then it modifies field n_trust in the same manner as p_truste. Each node updates it by including the trust value of the node from which it received the packet. So when node x receives RREP packet from y, it updates n_trust as:

$$n\_trust = n\_trust + Txy \quad (6)$$

Then intermediate node forwards the RREP packet along the route in source route of RREP packet. If an intermediate node overhear a RREP packet and it is not the intended next recipient, then it adds the first node in source route of RREP packet to neighbor table. The first node in source route is the one hop neighbor of destination.

3.5 Path decision at source node

When the RREP packet reaches the source node, the most secure path is selected by it. It calculates the path trust based on the trust values p_truste and n_trust received in the RREP packet and the number of nodes in the path. The path selected is the one which has the maximum path trust. Trust value of i^{th} path:

$$path\_truste_i = ((p\_truste + n\_trust) / 2) * w_i \quad (7)$$

where $w_i = 1 / n_i / \Sigma\, 1 / n_{i\,(i = 1 \text{ to } n)}$

$$path\_truste_{\,source - des} = \max(path - trust_i) \quad (8)$$

where:

n_i is the number of nodes in i^{th} path.
n is the total number of paths from s to d.
w_i is the weight assigned to the i^{th} path.
$path\_truste_i$ is the trust value of the i^{th} path.
$path\_truset_{source\text{-}des}$ is the trust value of the path selected as the most trust-worthy path.

4. Performance of Mobility assisted node reputation scheme for MANET Security

4.1 Simulation Environment

Network Simulator (2.3.2 version) is used to evaluate the effectiveness of the proposed method. Different scenarios are defined in a 600 * 600 Sqm with 40 mobile nodes. The source and destination nodes are randomly selected. In each scenario, each node moves in a random direction using the random waypoint model with a speed randomly chosen within the range of 0–25 m/s. The transmission range of each node is 150 m. It is assumed that there are nearly 25% malicious nodes are available in the ad hoc network.

4.2 Parameters for Evaluation

To evaluate the performance of the proposed scheme, the following metrics are used: Percentage of detection: It is defined as the ratio of the number of nodes detected as adversary and the actual number of such nodes present in the network.

Neighbor Node Communication Rate: It is defined as the time number of RREQ packets transferred taken to find a secure path from source to destination, in the presence of adversary nodes.

Throughput: it is the ratio of the number of data packets received by the destination node to the number of packets sent by the source node.

The results for the proposed scheme MNRS are compared with those obtained from reactive routing protocol DOA. DOA is the integration of DSR and AODV reactive routing protocols, by varying the number of adversary nodes in the network. Figure1 shows the number of node reputation consistency rate vs adversary node. As the number of adversary nodes increases node reputation consistency rate also increased. So more number of nodes means a high steep in the consistency rate. Figure 1 show that MNRS is able to detect more adversary nodes compared to trust based multi path reacting routing node. MNRS is able to explore more routes to destination as packet to be requested packet is unicasted. Therefore more number of paths is available at source and trustworthy path is selected based on the path trust. The percentage of detection is less than 100 due to node mobility which results in link breakage. When there is a link breakage the next trustworthy path is selected. But the behavior of some node may change during this time and it may start misbehaving. This information is available only with the intermediate nodes, which are unable to make any routing decisions. Thus the path selected may include such nodes, which remain undetected.

Table 3 shows that the adversary nodes of MNRS are more than DOA when there are no adversary nodes in the network. In MNRS a request packet is processed if the packet is received from different paths whereas in DOA a node drops the packet if it has seen it previously no matter for the path. But as the number of nodes increases in the packet the packets dropped which induces new route.

Table 3 Node reputation consistency rate vs adversary node

No. of Adversary Node	3	5	7	9	11	13	15	17	19	21
Node reputation Consistency Rate for DOA	4	6	8	9.5	10	10.5	11	11.5	12	12.5
Node reputation Consistency Rate for MNRS	7	9.2	11.2	12.3	13.0	13.5	14.2	14.5	15.3	15.4

Table 4 No. of Neighbor Node communication rate vs No. of adversary nodes

No. of Adversary Node	2	4	6	8	10	12	14	16	18
No. of Neighbor node communication rate for DOA	20	20.25	20.5	20	18	16	14	12	10
No. of neighbor node communication rate for MNRS	23	23.15	23.25	22	22.5	19.5	17	15.25	13

Table 5 No of neighbor node Diverted rate vs No. of adversary nodes

No. of Adversary Node	2	4	6	8	10	12	14	16	18	20
No. of Diverted Path for DOA	12	14	16	18	20	22.5	25.25	30	35	40
No. of Diverted Path for MNRS	19	21	23	25	27	29.5	32.25	37	42	47

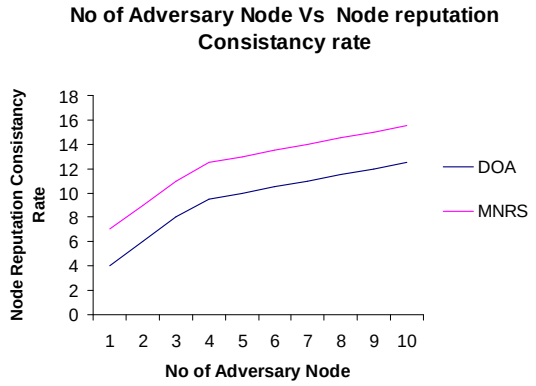

Fig. 1: Node reputation consistency rate vs adversary node

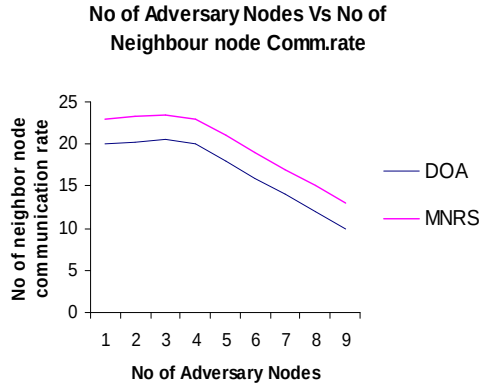

Fig. 2: Number of neighbor node communication rate Vs Number of adversary nodes

Fig. 2 and Table 4 show that the adversary nodes of MNRS are more than DOA when there are no adversary nodes in the network. In MNRS a request packet is processed if the packet is received from different paths whereas in DOA a node drops the packet if it has seen it previously no matter for the path. But as the number of nodes increase, the packets dropped which induces new route. In MNRS adversary nodes are detected and excluded from the path. The route discovery is delayed which indirectly decreasing the routing overhead. Unlike DOA approaches, which are based on broadcast of request, the scheme uses unicasting of route discovery packet from one hop neighbor of destination. This unicasting of rate of request introduces very less additional routing overhead on standard DOA in the network. The throughput of MNRS is more compared to DOA and reputation count. Throughput for all the methods degrades with the increase in number of adversary nodes in the network as shown in Figure 3and Table 5. It shows the number of adversary nodes vs number of diverted paths. However, the increase is steeper in reactive routing as it discovers the shortest path without detecting any adversary nodes which induce packet drop, excluding adversary nodes. It is clear from the graph that as the number of adversary node increases the number of diverted path also increases.

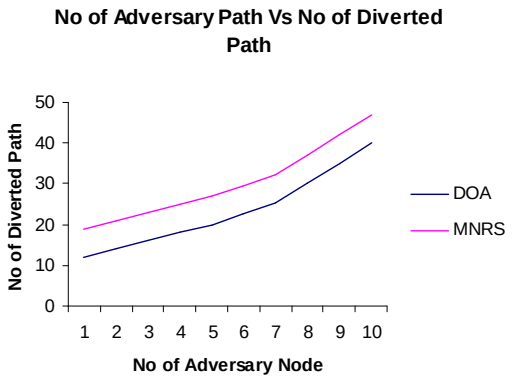

Fig. 3: No. of adversary nodes vs no. of diverted paths

5. Conclusion

The MNRS for secured MANET presented in this paper maintains the consistent knowledge about the node's communication spree, whether trusted or untrusted one. The proposed reputation scheme is used in improving the efficiency of overall network data transfer between different nodes. The neighbor node utilization rate is used to evaluate the consistent nature of nodes reputation behavior and minimize the route discovery delay threshold. Path diversity metric used in the simulation experiments for analyzing the MNRS shows the nature of data transfer route in the MANET reactive routing protocol.

The node's trustworthiness is very much used in sharing the information within the ad hoc network for secured data transfer in adverse conditions. Mobile nodes information uncertainty is handled with the mobility characteristics and its reputation is evaluated to trust or discard the node's communication. Simulations result shows that the performance of mobility based node reputation scheme in terms of nodes consistency behavior, neighboring communication rate, and path diversity compared to the reactive routing protocols are improved. The performance of the certainty reputation system improves and the average uncertainty increases even the percentage of misbehaving nodes increases.

References

[1] S. Kamvar, M. Schlosser and H. Garcia-Molina, "The Eigen trust Algorithm for Reputation Management in P2P Networks", Proceedings International Conference World Wide Web, http://kamvar.org/assets/papers/eigentrust, 2003.

[2] S. Buchegger, and J. Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes— Fairness In Distributed Ad hoc NeTworks", In Proceedings of ACM Workshop Mobile Ad Hoc Networking and Computing (Switzerland), doi: 10.1145/513800.513828, pp. 226-236, 2002.

[3] C.Boyd, A. Josang, and R Ismail, "A Survey of Trust And Reputation Systems for Online Service Provision", Preprint of article published in Decision Support System, DOI: 10.1016/j.dss.2005.05.019, Vol. 43, No. 2, pp. 618-644, 2007.

[4] W. Zhang, S. Das, and Y. Liu, "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks," Proc. 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communication and Networks, Vol. 1, pp. 60-69, 2006.

[5] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security, pp. 107-121, 2001.

[6] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks", Technical Report Stanford Univ., arXiv:cs/0307012v1 [cs.NI], 2003.

[7] S. Buchegger and J. Boudec, "A Robust Reputation System for P2P and Mobile Ad-Hoc Networks", In Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, citeulike:422300,2004.

[8] A.Pirzada, A., Datta, A. and McDonald, C., "Trustbased routing for ad-hoc wireless networks", In Proceeding of IEEE International Conference Networks (Singapore), DOI: 10.1109/ICON.2004.1409162, Vol. 1 pp. 326-330, 2004

[9] A. Josang, S. Marsh, and S. Pope, "Exploring Different Types of Trust Propagation", In Proceedings of the 4th International Conference on Trust Management (iTrust) Pisa, 2006.

[10] Poonam, K Garg, and M. Misra, "Trust based multi path DSR protocol", In Proceedings of Fifth International Conference on Availability, Reliability and Security, (Poland, February), DOI: 10.1109/ARES.2010.87 pp. 204-209, 2010.

[11] Wang, C., Yang, X. and Gao, Y., "A Routing Protocol Based on Trust for MANETs", In Proceeding of Sixth Annual International Conference on Grid and Cooperative Computing (Beijing, China), Lecture notes in computer science 3795, pp. 959-964, 2005.

[12] J. Wu and F. Dai,, "Mobility Management and Its Applications in Efficient Broadcasting in Mobile Ad Hoc Networks", Proceedings on IEEE INFOCOM, DOI: 10.1109/INFCOM.2004.1354507, 2004.

[13] J. Wu, S. Yang, and F. Dai, "Logarithmic Store-Carry-Forward Routing in Mobile Ad Hoc Networks", IEEE Trans. Parallel and Distributed Systems, Vol. 18, No. 6, pp. 735-748, June 2007.

[14] S. Capkun, M. Cagalj, and M. Srivastava, "Securing Localization with Hidden and Mobile Base Stations", Proceedings INFOCOM 25th IEEE International Conference on Computer Communications, DOI: 10.1109/INFOCOM.2006.302,2006.

AUTHOUR'S BIOGRAPHICS

A. Suresh, Research Scholar of Anna University, Chennai, is working as an Associate Professor at K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu. He has completed his Bachelor's Degree (Mathematics), Masters Degree (M.C.A.) at Kandasamy Kandar's College, Affiliated to University of Madras, Tamilnadu and M.Phil at Manonmanium Sundharanar University, Tirunalveli, TamilNadu. His research interests include Mobile Adhoc Networks.

K Duraiswamy received the B.E., M.Sc. and Ph.D. degrees, from the University of Madras and Anna University in 1965, 1968 and 1987 respectively. He worked as a Lecturer in the Department of Electrical Engineering in Government College of Engg, Salem from 1968, as an Assistant professor in Government College of Technology, Coimbatore from 1983 and as the Principal at K. S. Rangasamy College of Technology from 1995. He is currently working as a Dean in the Department of Computer Science and Engineering at K. S. Rangasamy College of Technology (Autonomous Institution). His research interest includes Mobile Computing, Soft Computing, Computer Architecture and Data Mining. He is a senior member of ISTE, IEEE and CSI.