TRUST EVALUATION ALGORITHM (TEA) TO IDENTIFY MALICIOUS NODE IN MANET

L Raghavendar Raju[1], M Praveen Kumar[2]
[1]Assistant Professor, Dept of CSE, Matrusri Engineering College, Hyderabad, India,
[2]Assistant Professor, Dept of CSE, Matrusri Engineering College, Hyderabad, India,

Abstract: MANET is less resistant to malicious node more prone to selfish behavior of nodes and compromised nodes which are most often undetectable. Due to resource constraints and high mobility characteristics. In a clustered network one of the cluster member is chosen as a cluster head. But if the selected node becomes selfish or malicious, it will affect the performance of the entire group communication. This paper proposes a Trust Evaluation Algorithm (TEA) to identify the nodes with highest level of trust within the cluster. The nodes are added to the trust table based on the calculated trust level. The friends having highest trust level is eligible to become cluster heads. Among the available cluster heads, one among them is selected as the cluster head.other nodes are considered as a cluster members. The nodes with least trust values are regarded as malicious and are removed from the list and are stored in a noticeable unwanted record. Our TEA approach succeeds in achieving high resistance towards network attacks.

***Index Terms*-- MANETs, QoS Trust, TRUST, Cluster Head.**

I. INTRODUCTION

MANET is a set of self-organizing portable hosts equipped with wireless communication devices collected in groups with no need for fixed structure and centralized administration to form a network of radio links. Each the mobile node can act as a host and a router independently using the wireless medium within the communication range to manage the communication between large numbers of individual mobile nodes by dynamically forming a communication network and exchange the data among them without utilizing any established set of base station [2]. Trust is interpreted in respect of the confident relation of one node to the rest of the nodes [3, 4] which is a vector that is computed on the grounds of nodes behavior when necessary and used for how to decide about the feature of nodes and their work is done, and how to give the equivalent route approach control based on its neighbor communication status then build authority for each node by watching the behaviour of nodes. A trusted technique mentions, computes and makes trust connection among nodes. Trust management based routing is used to restrict many attacks like wormhole attack, black-hole attack, denial of service, selfish attack, etc. Trust can be constructed in many ways by reputation, subjective logic and from an opinion of neighboring nodes. There is two types of trust are available such as direct trust and indirect trust. Immediate trust is first-hand information for neighbors and easy to be obtained. Indirect trust is second-hand information about nodes termed as recommend trust which is obtained from a third party or neighbouring nodes[5] [6] [7]. Characteristics of MANET such as dynamic topology changes, absence of base station and ease of joining or leaving the networks at any time makes the ad hoc networks into more prone to physical security threats and difficult to ensure that a packet has been delivered to the correct destination so there is need to provide secure communication and to reduce the hazards from malicious nodes by incorporating the trust into MANET. An adversary node is eager to add in network and disrupt the routing process by dropping the packets it receives for forwarding, i.e. denial of service, to sincerely cooperate in the routing procedure. Damaging the routing process involve revealing private data, packet modification, under wrapping message and pretend to be another nodes, hence breaching the common safety requirements. So malicious attacks on an MANET can evolve from both inside and outside the network and target at any node all this implies that each basic node must be ready for an attack with an protection directly or indirectly. For that trusts base routing based on trust node evaluation results furnishes excelling throughput boost [8]. Considering the aid of trust technique mobile nodes can justify at what level they can trust other mobile nodes to prevent most dangerous behavior, such as acquiring or disbursing packets from and to the host with less trustworthy levels.

II. RELATED WORK

Hui Xia et al [9] developed trust predication model (TSR)called as source routing protocol based on trust, to select the lesser length route as the forwarding path that satisfied the transmission of data packets accurately considering method based on prediction logic rules and on nodes historical experience. Neighbour considered as a malicious node is stored in the black list of the observing node by comparing its trust with the trust threshold of black-list. In which a source launched many multiple loop-less routes to a destined node in one route discovery process, and every route obtains a \calculated value consisting of count based on Hop and route trust value. A destined node replied with an optimal trustworthy routes as qualified routes to the source that satisfied the trust requirements of transmitting data packets.

Ahmed M. Abd El-Haleem et al [10] designed model based on trust in which the relationship among various nodes is calculated by score considering the trust factor that consisting of direct and indirect trust and cooperation score depending on the beta probability density function. Algorithm used data link layer acknowledgement and transmission control end-to-end protocol acknowledgement as tools to watch the behaviour of nodes which updated the value of trust of neighbour definite or indefinite according to its data transmitting to its neighbouring nodes and loss of data packets behaviour. Cooperation score is used to identify the selfish ness behaviour of a suspicious node and restrict the granted degree of node malicious behaviour for defining exact trusted and non trusted node to route across the node that misbehaves.

Zhexiong Wei et al [11] modeled trust management scheme using uncertain reasoning for improving the security in MANETs. The security is obtained by evaluating trust value by joining both the algorithm that is observation through direct method and indirect method. With direct analyzation technique the trust value of a node is obtained with the help of Bayesian inference considering the total probability model to be illustrated by direct method. using indirect observation considering neighbour nodes of the node which observes, by the help of Dempster-

Shafer theory the trust value is obtained when the proposition of interest to be achieved by an indirect method and updated the values after storing the values in the module of trust table. Routing techniques in the wireless network selected the nodes with low trust values to build safe routing paths between sources and destinations from the trust repository module.

III. PROPOSED METHODOLOGY

In a given, cluster-based network cluster head is chosen [12]. Considering the elected nodes as leaders of the group and other remaining nodes as leaf nodes a tree of multicast nature [13] of the shortest path is established. Finally, the data is routed to the destined cluster or node[1] If the selected cluster head become selfish or malicious, then the performance of the whole group communication will change. Hence only the nodes with the highest level of trust should be elected as cluster heads.

The trust management is encouraged using collaborative trust-based routing protocol for MANETS [9]. The direct interactions with the neighbors are evaluated based on the number of honest attempts made by the node. The level of honesty the user posses is based on its actions are recorded in a trust table. Thus the trust value is allotted to a node which is obtained with the help of neighbors direct interaction and the suggestions from its neighbors. Along with this behavior based trust, the QoS trust metric [15] is considered such as the energy level and degree of being cooperative of each node in data transmission. The nodes are then added to the friend list based on the trust level. The friends having highest trust level are eligible to become cluster heads.

In this paper, we are proposing an algorithm to evaluate the nodes trust value considering direct interaction with its neighbors. In this technique, each node challenges it's 1- Hop neighbors and formulates a trust value. The network consists of a sender node S and multiple member nodes (20 nodes are considered). As these nodes are arbitrary in the given environment, at first they are not in any connection with their neighbor nodes. Consider a network where four clusters are formed randomly with multiple nodes in each cluster. From the given arbitrary network with multiple malicious nodes the first task of our proposed algorithm is to select the cluster member. The Hello message will be transmitted by a cluster member node to its immediate neighbours. The Hello message structure frame is as shown in the following Figure 1[12].

TABLE 1: Structure of hello Message

Message Header				
S ID	Seq.No	Residual energy	BW	Connectivity

Hello message contains the source id of the sender node along with the key parameters like residual energy, bandwidth and connecting of the sender node to its neighbor nodes.

As all the nodes in a cluster (example cluster1) would broadcast Hello message to all its immediate neighbors, each nodes in the cluster has the information about its immediate nodes in the network. During the Hello message transmission and reception, direct trust value of each node is calculated.

$$DirectTrust = \frac{No.ofPkts\,Received}{No.ofPktsSent}$$

Direct trust value is calculated at every node for its immediate 1-Hop neighbor node as shown in Figure 1. *Hello* packet sent by the sender node *is* also re-transmitted to the same node. Using the ratio of total quantity packets send from a node to its immediate neighbor to the total quantity of *Hello* packets received back from the same immediate node. Since the obtained DT value is a floating point value, it requires more storage space hence $ceil(DT*10)$ is considered to obtain an integer value.

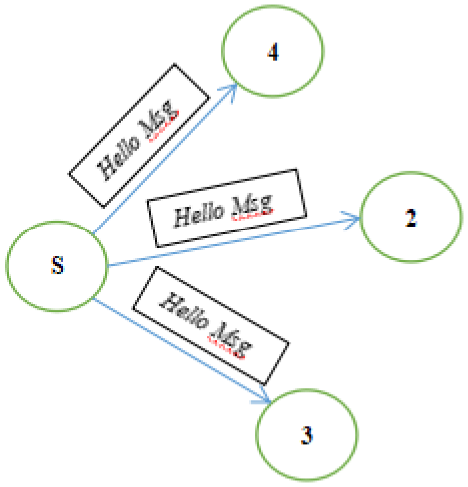

Fig 1a

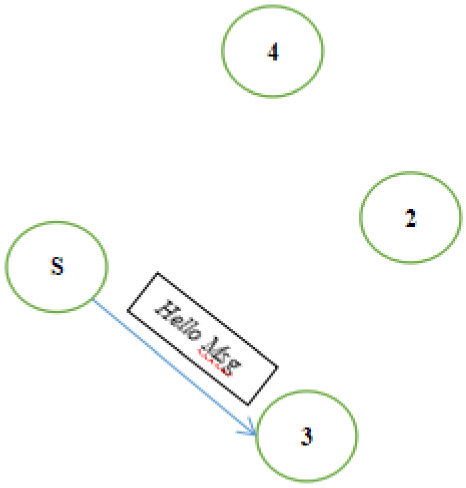

Fig 1b

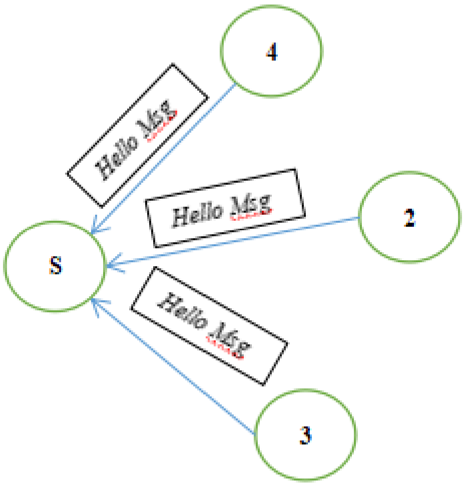

Fig 1c

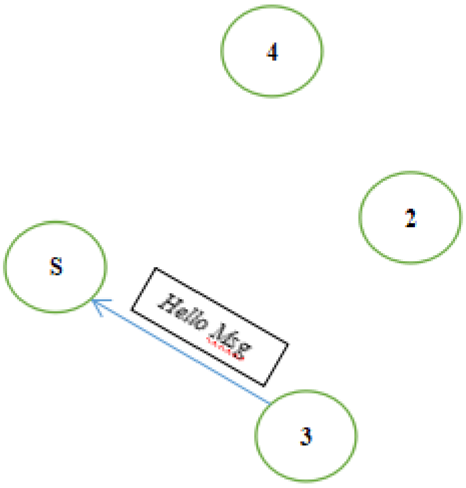

Fig 1d

Trust Table	
Node	**Trust Value**
4	1
2	1
3	?

Trust Table	
Node	**Trust Value**
4	1
2	1
3	0.5

Figure 1: Trust evaluation using *Hello Message* transmission ,(a) node broadcasts *Hello Message* (b)Reception of *Hello Message* from node 2 and node 4's *Hello Message* broadcast (c) rebroadcast of *Hello Message* from node 1 (d) Node 1 receives *Hello Message* from Node 3.

A *DT* value of 0.65 would yield [*ceil*(0.65*10)] value 7. To reduce the storage space four bit space of memory is sufficient to store the data .Since the energy consumption at every node is considered to be depending on the quantity of bits transmitted, our algorithm will drastically deduce the consumption of energy and reduce the overhead occurred due to communication between the nodes.

During direct trust evaluation the trust value of each node is assigned a value in the interval $0 < ceil(DT *10) \leq 10$ .The node that has a lowest *ceil*(*DT* *10) is isolated during group communication.

The proposed TEA evaluates the neighbour by helping in establishing trust for a node with respect to the other node existing in the MANET. In turn it authenticates the nodes by performing a unique integrity test on a node to prove its honesty in the network with respect to its neighbouring nodes.

A)Trust Evaluation Algorithm for the neighbouring nodes:

At this stage, every node is provided with two values of distinct prime numbers of large integers .

For example consider node *A* with secret pair of prime integers (*a*,*b*) and node *B* with secret pair of prime integer's (*c*, *d*).Whenever a mobile node wishes to transmit a challenge to a particular identified node, it chooses one of the many prime number (' *n*') randomly and waits for a answer back from the node.

Considering the situation where nodeA and nodeB are challenging between themselves:

STEP1: *Assign (a,b) nodeA and assign (c,d) to nodeB*

STEP2: *nodeA challenges node B , by sending a random prime number ' n ' using R-REQ packet. (as shown in Table 2).*

STEP 3: *nodeB computes cd mod n and sends its result through all the possible paths (broadcasting) using R_REP packet (As shown in Table 3)*

STEP 4: *node A compares the result obtained to it through multiple paths and arrives at a decision at node B .*

As predicted *n* , *c* and *d* are huge prime numbers, it is difficult to identify *c* and *d* from the calculated value of the *mod* arithmetic function (since the value of mod function ranges in the interval [0, *n*]).

As known about Grey Hole Attack, they always tens to modify the data packets hence during the process of challenging a nodes neighbor node, such a malicious node always alters the value of *cd* mod *n* in R_REP. When the source node finds difference in the values of the computer *cd* mod *n* the route with the most distinct value is not considered and the nearest neighbor node I that path is considered as malicious node and is assigned the least trust value and is eliminated from the friend list.

Table.2. R_REQ message frame

R_REQ Message			
Source ID	Sequence No.	Destination ID	Arbitrary Prime 'n'

Table.3. R_REP message frame

R_REQ Message			
Destination ID	Sequence No.	Source ID	C^d mod n

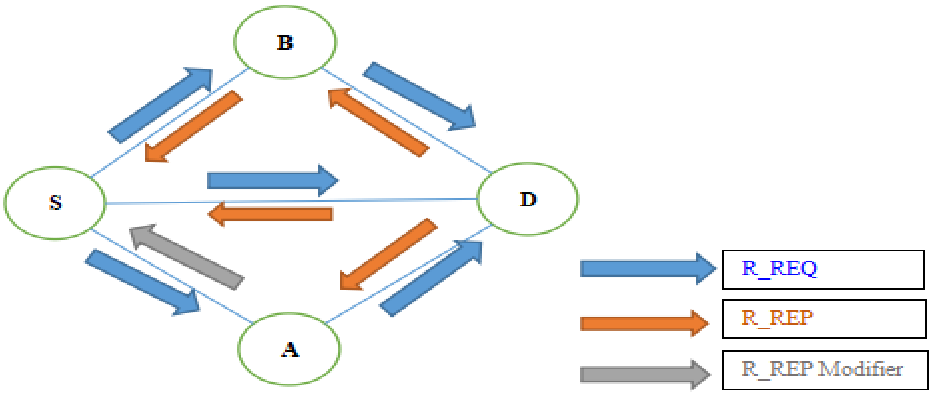

Fig.2. Evaluation for one-hop neighbor node

For example (as shown in Figure 2) consider node S broadcasting R_REQ to node D, but obtaining similar R_REP from two routes and a modified R_REP from third route. Hence the sender node compares all the R_REP for *cd* mod *n* value. The route which provides a modified value of *cd* mod *n* is considered to have a malicious node. Hence the node in the path (node A) is considered as an attacker and hence is excluded from the friend list.

IV.CONCLUSION

In a Clustering Algorithm for MANET for each cluster one node is elected as cluster node for communication with other cluster members. But if the chosen node becomes selfish or

malicious node, it will modify the the entire group communication performance. Hence only the nodes with highest level of trust are elected as cluster heads. In direct trust management the nodes trust value is calculated depending on the direct interaction with its neighbors. The Trust Evaluation Algorithm for the neighboring nodes identifies the malicious node and excludes it from the friend list for the communication within the cluster.

REFERENCES

[1] Sapna B Kulkarni, Dr.Yuvaraju B N, “Node connectivity, Energy and Bandwidth Aware Clustering Routing Algorithm for Real-time Traffic Multicasting in MANET”, 2015 IEEE International Advance Computing Conference number #35547, paper is indexed in IEEEXplore Digital Library, Xplore Complaint ISBN:978-1-4799-8047-5/15@2015 IEEE.

[2] Naveen, N., A. Annalakshmi, and K. R. Valluvan. "Trust node valuation and path reliability technique for intrusion detection in MANET." In Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on, pp. 468-472, ISSN: 978-1-4673-5845-3, IEEE, 2013.

[3] R. Menaka1, and V. Ranganathan, “A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, vol. 3, Issue 4, April 2013.

[4] Hui Xia, ZhipingJia, Lei Ju, Xin Li, and Youqin Zhu, “A Subjective Trust Management Model with Multiple Decision Factors for MANET Based on AHP and Fuzzy Logic Rules”, 11 Proceedings of the IEEE/ACM International Conference on Green Computing and Communications, pp. 124-130, 2011.

[5] Sardar,Mousumi, and KoushikMajumder, "A Survey on Trust Based Secure Routing in MANET", Computer Science, pp. 243–253, 2013.

[6] Almotiri, Sultan, and Irfan Awan, "Trust Routing in MANET for Securing DSR Routing Protocol", 2010.

[7] Li, Xin, ZhipingJia, Peng Zhang, and Haiyang Wang. "A Trust-Based Multipath Routing Framework for Mobile Ad Hoc Networks." Seventh International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2010, vol. 2, pp. 773-777. IEEE, 2010.

[8] Yan, Zheng, Peng Zhang, and Teemupekka Virtanen. "Trust evaluation based security solution in ad hoc networks." In Proceedings of the Seventh Nordic Workshop on Secure IT Systems, vol. 14. 2003.

[9] Xia, Hui, ZhipingJia, Xin Li, Lei Ju, and Edwin H-M. Sha. "Trust prediction and trust-based source routing in mobile ad hoc networks,Ad Hoc Networks 11, no. 7, pp. 2096-2114, 2013.

[10] El-Haleem, Ahmed M. Abd, Ihab A. Ali, Ibrahim I. Ibrahim, and Abdel Rahman H. El-Sawy. "Trust model for TRIDNT trust based routing Protocol", 2nd International Conference on Computer Technology and Development (ICCTD), pp. 538-544, IEEE, 2010.

[11] Wei, Zhexiong, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", 2014.

[12] Sapna B Kulkarni, Yuvaraju BN “ENB Cluster Head Selection Algorithm for MANET”, “International Journal on EngineeringTechnology and Sciences(TM) (IJETS)", Volume-2, Issue-1, and January 30, 2015.

[13] Sapna B Kulkarni ,Yuvaraju BN , “Shortest path Multicast tree construction algorithm to transmit multimedia real time traffic in MANETS”, ”International Journal of Innovation and Advancement in computer science(IJIACS),ISSN-2347-8616,Volume 4 special issue March 2015(ICETESMA-15,JNU University, New Delhi)

[14] Sapna B Kulkarni, Yuvaraju BN, ”The Top-N rule selection approach algorithm to split the multimedia traffic stream into multiple substreams prior to transmission in MANETS”, IPASJ International Journal of Computer Science (IIJCS), Volume3, Issue1, January2015.

[15] Jin-Hee Cho, Ananthram Swami and Ing-RayChen, “Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks”, Journal of Network and Computer Applications, Volume 35, Issue 3, May 2012, Pages 1001–1012.