TRUST ASSESSMENT THROUGH FTA APPROACH IN AD-HOC NETWORK

Ananya Banerjee[1], Sutanu Ghosh[2] and Anirban Neogi[3]

[1,2,3] Dr.Sudhir Chandra Sur Degree Engineering College; Kolkata 700074.
ananya.banerjeee@gmail.com, sutanu99@gmail.com,
anirban_neogi@yahoo.com

ABSTRACT

An Ad-hoc network consists of communicating nodes to establish improvised communication with environment without any fixed infrastructure. Nodes in Ad-hoc network (MANET) do not rely on a central infrastructure management but relay packets sent by other nodes. Mobile ad-hoc network can work properly only if the participating nodes collaborate with routing. Therefore it is required that the nodes co-operate for the intensity of operator network. Because of the high mobility of the nodes in the network, detection of misbehaviour of any node is a complex problem. Nodes have to share the routing information in order for each to find the route to the destination. This conceptual paper is based on the relationship among the nodes which makes them to co-operate in an ad-hoc network .This require nodes to Trust each other. Thus we can say Trust is a important concept in secure routing mechanism among the nodes. In this paper we present a unique Trust based method in which each node broadcast a RQ packet if it is received from different neighbours. The secure, efficient and reliable route towards the destination is calculated as a weighted average of the Trust value of the nodes in the route, with respect to it's behaviour observed by the neighbour nodes and the number of nodes in the route.

KEYWORDS

DSR, Trust enhancement, correlation among neighbour nodes, malicious nodes, throughput, FTA, OPI, routing overhead.

1. INTRODUCTION

The nodes are usually mobile portable devices, self organised and any sort of end to end communication between them requires routing of information via several intermediate nodes. A mobile ad-hoc network (MANET) is the collection of wireless mobile nodes to establish a temporary connection neither in a predefined way nor using a static network structure. Due to the lack of infrastructure and limited transmission facility of a node in a mobile ad-hoc network, a node has to rely on neighbour nodes to send a packet to the destination. Since routing is a basic service in such network and a prerequisite for other services, it has to be reliable and trustworthy. Recently, the routing protocols for mobile ad hoc network, such as DSR and AODV are based on the assumption that all nodes will co-operate. Without co-operation no packet can be forwarded to the desired destination and hence no proper routing is possible.

There are two types of non co-operative nodes can be classified: i) faulty or malicious node and ii) selfish node. Both of these are misbehaved nodes. Misbehaviour means to attempt the benefits from other nodes but to refuse to share it's resources. So with these misbehaved nodes both DSR and AODV may not result the proper routing. Enforcing the co-operation among the

Rupak Bhattacharyya et al. (Eds) : ACER 2013,
pp. 295–304, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3228

mobile nodes is particularly challenging which may solve for many routing issues. In this paper a modified approach for optimising the routing protocol through assessing the trust level between nodes is introduced. Different scenarios are identified and are combined simulated to determine if anode is action maliciously or not.

2. Earlier Work For Trust Enhanced Route For Ad-Hoc Networks

In the DSR protocol, DSR routing model faces some security problems, those are given below:

a) Through the non jam-packed route, RQ packets reach the destination very soon rather than the jam packed route. So jam-packed route can be avoided. But there is a problem that is a shorter path may present within the jam-packed route which may not be utilised.
b) The one hop neighbour sends RQ packets to the destination end , just after receiving 1st RQ.As a result most of the packets from the other nodes(far from destination node) are discarded.
c) A node, after receiving RQ packet, checks it and drops it if it is previously processed. As a result a malicious node forwards that RQ very quickly, then the other RQ packets from the other nodes, are dropped.
d) Sometimes malicious node hampers good traffic operation in an ad-hoc network by disturbing route error information, routing table, routing state etc.

In order to solve these above mentioned problems and to establish a robust secure reliable path from source to destination without falsification of route and information packet we are going to introduce Trust Enhancement Route scheme for ad-hoc network.

Trust value: Reliability, of a node with respected to its neighbour node can be represented by a parameter, called trust value of a node in a network. *An initial* Trust value is assigned for neighbour node which is encountered for the 1st time. Initialisation of assignment of the initial trust value of the neighbour nodes including malicious nodes can be done by the trust values of known neighbour nodes. Actually a Trust value depends upon the experience of given node.

Up gradation of trust value: The Trust value for a neighbour node will be upgraded, when a node gets the RP packet from this neighbour node. So there should be a function to upgrade the Trust value:

$T(next)=K[T(previous)-Ex]+Ex$**.**

Where, T(next)=New upgraded Trust value. T(previous)=previous Trust value, Ex = value of experience, K = constant

There are two sub modules under this module:

- Administrator module which is use to accumulate Trust information of the known nodes. It acts as a interface between DSR protocol and previous modules.
- Router module selects the most reliable path having lowest number of malicious nodes, depending upon the Intimacy of a node with its neighbour nodes.
-

De gradation of trust value: If the RP packet is not received, the Trust value for this neighbour node has to be de graded.

Establishment of the co-relation of the neighbour nodes:

If the trust value of the neighbour node is greater than a threshold value then that node is a known node for the source node, otherwise it is an unknown node for the source node. This threshold value can be represented by a numerical value i.e., 0.5.

This known node is classified into two categories i) Completely known and ii) Moderately known.

Table 1. Co-relation table

Relation with source	**Trust value**	**Transaction type**
Completely known node	T_c: $0.75<T<=1$	Plenty of reception RP and transmission RQ of packets
Moderately known node	T_m: $0.5<=T<0.75$	Few transaction
Unknown node / Malicious node	T_u: $0<=T<0.5$	No transaction

When Trust value of a known node is greater than 0.5 and less than 0.75 then this is a moderately known node. That means the transaction between the source node and this neighbour node is performed moderately. And when Trust value of a known node is greater than 0.75 and less than 1 then this is a completely known node. That means lots of transaction are performed between source and this neighbour node.

2.1. For reliable transaction

First of all we should recognise the malicious node which is responsible to falsify the path detection and the information, to secure the transaction we can follow the above mentioned co-relation table. During source to destination data transmission we should include the important field that is Trust field at the header part of the framed packet along with the payload.

For one –way propagation there is a timer, $T_d = 2*R/s+K$.

Where R = maximum range for sending data.
s = speed of data which is transmitted.
K = constant.

After every RQ packet reception by a neighbour node, the Trust field of the data is updated by using a formula
Trust field (new) =Trust field (previous) + T_{xy} (when x node receives the broadcasted data of node y).

Similarly when the destination node receives the packet which is sent by the source and reaches at the destination through a reliable, shorted route, another trust field should be introduced at the header of RP packet, which will be transmitted to the source. For forward direction Trust field is denoted by T_f and for the reverse direction Trust field is denoted by T_r.

2.2. Total transaction

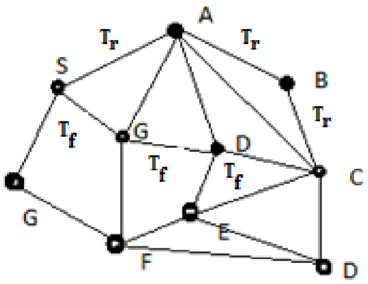

Fig. 1 : A Network

In a DSR network we consider source S sends data to the destination end D.In this Fig.1 S sends RQ packet to all the neighbours. A communication between S and C is shown here. In transmission path the packets routed through S, G, D and C and in reverse path it is routed through C, B, A and S. Nodes with T_f field along with the header to discover a secure path to destination. After selection of the secure, shortest path, let S sends packet through the path S, G, D and C to the destination end. Each and every intermediate node upgrades its Trust field by involving Trust values of the node from where it receives the packet. From source to destination RQ packet transmission the total Trust value has to be:

$T_f(total) = T(AS)+T(BA)+T(CB)+T(DC).$

After reception of the data packet from the source end, D sends an acknowledgement through a reliable path, therefore like an S node; D node also checks the Trust values of neighbour nodes within its path to source. So for RP packets the total reverse direction Trust value has to be:

$T_r(total) = T(CD)+T(BC)+T(AB)+T(SA).$

So for total transaction (From source to destination and destination to source), the total trust value can be calculated as

$T=[\{T_f(total)+T_r(total)\}/2]*S_i=[\{T(AS)+T(BA)+T(CB)+T(DC)+$
$T(CD)+T(BC)+T(AB)+T(SA)\}/2]*S_i.$

Where, $S_i=1/x_i/\sum_{i=1}^{X}1/x_i$, for ith possible path

Therefore from the above expression of **T** all nodes have mutual Trust information within the path from source to destination.

3. PERFORMANCE ANALYSIS IN OUR PREVIOUS WORK

We have used network simulator 2, a simulator for mobile Ad-hoc network to evaluate the effectiveness of the proposed scheme. The simulator is done with 25 nodes moving with speeds 1, 5, 10, 15, 20 m/s in a 400x400 sq.m. area. The pause time is 10 ms between the movements of the nodes. The transmission range of the each node is 100 m. We assume that there are 0-40% malicious nodes in the network.

To analyze the Performance of the proposed scheme we use the following metrics:

Routing Overhead: It is define as the number of RQ packets transferred taken to find a secure path from source to destination, in the presence of malicious 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 performance of the proposed scheme is compared with standard DSR protocol by varying the number of malicious nodes and node moving speed. For performance analysis we have used three parameters-

i) Routing overhead, ii) dropping of malicious nodes, iii) Throughput.

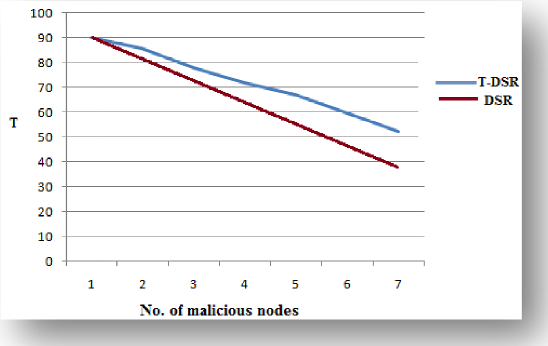

Fig. 2: Comparative graph of Throughput of T-DSR and DSR with respect to number of malicious nodes

In fig 2 the achieved throughput is clearly greater than the standard DSR.

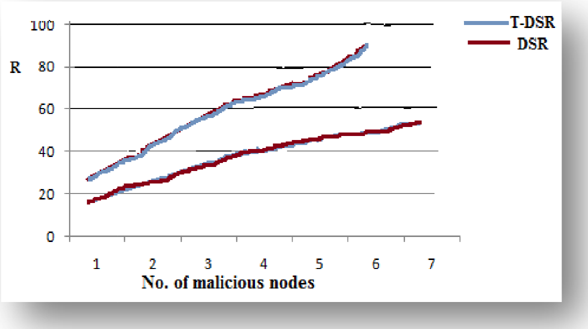

Fig. 3: Comparative graph of Routing overhead of T-DSR and DSR with respect to number of malicious nodes

The next observing parameter is Routing Overhead, which is clearly high compared to the standard DSR.

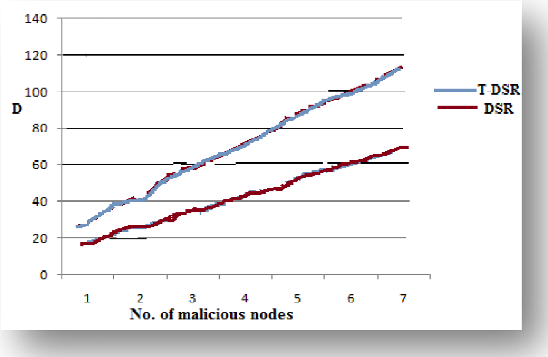

Fig. 4: Comparative graph of dropping malicious node of T-DSR and DSR

Fig. 4 shows the dropping of malicious nodes over total drops. The amount of dropping is less in case of Trust Enhancement scheme compared to standard DSR.

4. Overview Of The FTA

Trust Level in an ad-hoc network serves the reliability of nodes during data packets transmission from source to destination through a most reliable path. So we propose an algorithm based on fuzzy logic to evaluate trust value of the nodes, and at the same time this algorithm is used to recognise the malicious nodes in the network.

The input parameters of FTA are a) number of replay attacks, b) forwarded packets to the wrong destination, c) number of untruthful routing message, d) number of dropped packets.

In the undiscovered route if P (source) wants to send information packets to the Q (destination end), path discovery should be done on demand. First of all P sends RQ (route request signal) to its neighbouring nodes, those are responsible to find out the trust values of their next hop nodes. Here we consider the minimum trust level of kth node in nth route, is T_{nk} where k ϵ (1,....n).

To choose most reliable path from P to Q, FTA uses the trust values of nodes. In this protocol, after sending a RQ, P node can get more than one RP .Because of the source initiated on-demand routing protocol, the nodes which are not included in a selected path will not participate in routing table. Destination IP address, sequence no. flag, trust level, and hop count and information next hop should be included in FTA table.

When P starts to send a message to Q it starts to initiate a valid path between them by sending a signal RQ to its neighbours. the RQ consists of P’s IP address, its sequence no., its current trust value, hop count and life span .To with when the sequence no. is unknown the sequence no. flag must be set to some initial value and the hop count may be considered as 0.At the intermediate node the hop-count of RQ packet is increased by 1, and the hopping information towards the initialisation of the valid path between P and Q is updated. In the same way the trust level at the current node is compared with the previous one and updates the trust parameter in the trust field of originator RQ packet. In this way in each comparison whenever the present trust level is greater than the previous one the RQ packet is updated and hence moves towards a valid path.

In order to establish a reverse path each intermediate node records the address of neighbours from which they receive packets. Once RQ reaches the destination Q, a RP packet is generated and travels though the reverse path. Whenever an intermediate node receives RP it increases the hop count value by 1since RP is moving through a reverse path, when RP reaches the source, the hop-count indicates the double distance between the P and Q. The source sequence number in RP is compared with destination sequence number and compared at each node in order to conclude the current trust value. The minimum value represents the trust level of the route. FTA now picks the route with highest trust level as the most reliable path between P and Q.

5. Performance Analysis Of Trust Level Using FTA

We have started our analysis with the same network as in our earlier paper. We have used OPNER modeller V11.5 for the simulation. One wireless LAN with 25 nodes with speed 11Mbps within AODV routing protocol is considered. The simulation process consists of no. of scenarios producing practical configuration. Every scenario runs in 5 different configurations. For example, none of the above 25 nodes acts maliciously or 10 or 15 of them are acting maliciously and so on. We also have considered the malicious nodes drop packets within the simulation time. In our case each malicious nodes are dropping packets in between 50 and 100 seconds where as the total simulation is done within the span of 300 seconds. We also have said the condition that for the 1st 60 seconds the nodes move randomly with a speed 10 meter /sec, after that in duration of 20 seconds they come back to their initial position.

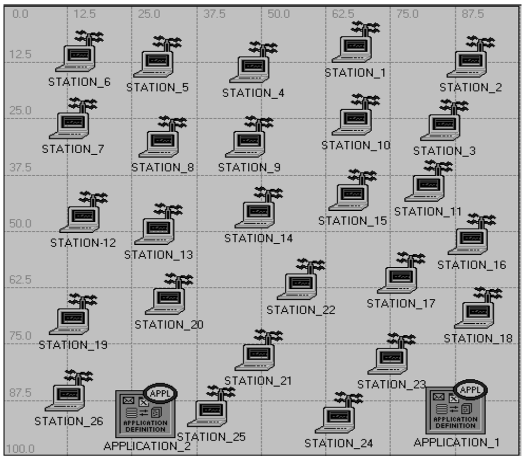

Fig. 5: Experimental Scenario

We choose our scenarios such that station _1 sends traffic to station _25.To study of the effects of the malicious node three performance matrix will be measured for their above mentioned scenarios namely Throughput (T), Routing overhead (R) and Drop of packet (D).To compare the performance of different approaches we define overall performance index defined as, $OPI=W_T*T+W_D*D+W_{Dl}*Dl$ where Dl represents round trip delay and W's represents corresponding weights.

The distribution of the weights can defer from one application to other, as an example for voice and video based application the weight for packet loss should have the highest value. In our case to study the ADHOC network we choose $W_T= W_d=25$ and $W_{Dl}=50$.

6. RESULTS AND ANALYSIS

The variation of the Throughput, Routing overheads and Drop of packets are analysing individually .in all the cases the performances are improved with FTA approach. In figure 5 it can be seen that T is improved by around 30% .Whereas the route over head is improved only 8-10 % because the network consists of 25 nodes. If the no. of node reduced down to 5, R may be improved up to 20-25%.The packet loss is maximum when all node starts to behave maliciously but it remain almost same in comparison with DSR and T-DSR. The following table makes a comparison between TDSR and FTA to establish the improvement of our proposed scheme.

Table 2. Comparative table of TDSR and FTA

Parameters	TDSR (in percentage)	FTA (in percentage)
Drop of packets	51	50
OPI	45.54	59.66

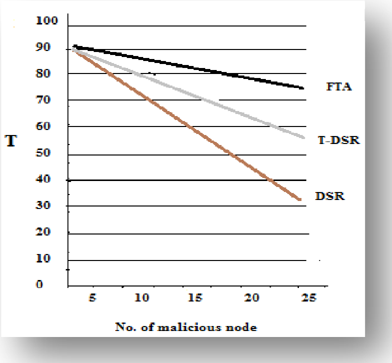

Fig. 6: Comparative graph of Throughput of DSR, T-DSR and FTA with respect to number of malicious nodes

In this figure throughput is better for FTA. The throughput of DSR decreases so fast than other two protocols.

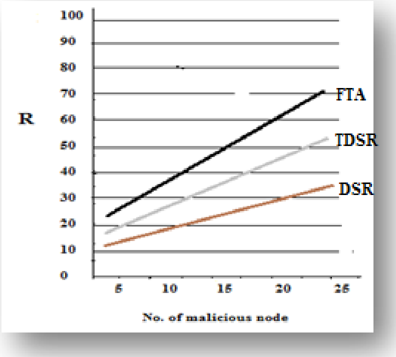

Fig. 7: Comparative graph of Routing Overhead of DSR, T-DSR and FTA with respect to number of malicious nodes

In the fig. 7 the routing overhead of FTA is much more than TDSR and DSR. The Routing overhead is close to 70 above for FTA in our experiment.

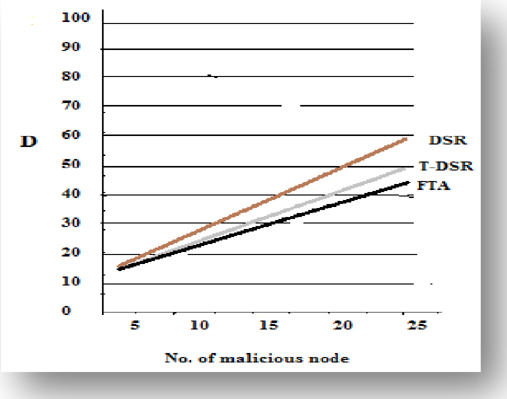

Fig. 8: Comparative graph of dropping malicious nodes of DSR, T-DSR and FTA

In the Fig. 8 the drop of the packets are much more less for the case of FTA.

7. Conclusion And Future Work

In this paper we have highlighted the significance of Trust Enhancement of the mobile ad-hoc network; we also analyze the different types of security issues to the network. The proposed scheme can be used to improve the reliability and the performance to an Ad-hoc network. Here we are using fuzzy logic concept for Trust Enhancement to solve the problem of lack of infrastructure in MANET. Significant improvement is been observed after applying the proposed scheme which will motivate us for some further improved performance analysis of Ad-hoc network. Further investigations in this regard can be carried out to prevent node congestion and to provide load balancing using alternate routes discovered by the proposed protocol.

References

[1] A.Neogi and A. Banerjee. “Trust Improvement among the nodes in a Wireless Ad-hoc Network” International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 3, May2012.

[2] Alia Fourati, Khaldoun Al Agha and Hella Kaffel Ben Ayed “Secure and Fair Auctions over Ad Hoc Networks” Int. J. Electronic Business, 2007.

[3] Jeremy J. Blum, Member, IEEE, and Azim Eskandarian, Member, IEEE, “A Reliable Link-Layer Protocol for Robust and Scalable Intervehicle Communications” IEEE Transactions On Intelligent Transportation Systems, vol. 8, no. 1, March 2007.

[4] Huaizhi Li and Mukesh Singha, “Trust Management in Distributed Systems” IEEE Computer Society February 2007.

[5] C.Shiva Ram Murthy and B.S.Manoj, “ ad hoc wireless network: Architecture and Protocol” Prentice Hall,2004.

[6] D.Johnson, D.Maltz, Y.Hu and J.Jetcheva, The DSR protocol for mobile ad hoc network, Internet Engineering Task Force, Mar.2001. http://www.ietf.org/internetdrafts/draft-ietf.

[7] Richard Dawkins. The selfish Gene. Oxford University Press,1980 edition.1976.

[8] S.Murthy,” Routing Protocol threat analysis” Internet Engineering Task Force, Mar.2002. http:/www.ietf.org/internetdrafts/draft-ietf.

[9] Ernesto Jimenez Caballero, “Vulnerabilities of Intrusion Detection System in Mobile Ad hoc network- The routing problems”, Tkk t-110.5290 seminar on Network security 2006.

[10] Y.C.Hu, A.Perring and D.B.Johnson," Packet Leashes: A Defence against Wormhole attacks in wireless Ad hoc network", Proc. 22nd annual joint conference . IEEE computer and communication society (Infocom 03) Sanfransisco,CA, April'2003.

[11] Sonja Buchegger and Jean-Yves Le Boudec ," Performance analysis of CONFIDANT Protocol", Proceedings of the 3rd ACM International symposium on mobile Ad hoc networking and computing'02.

[12] John Keane, " trust Based DSR in Mobile Ad hoc networks, Trinity College Dublin,2002.

[13] Kevin Fall and Kannan Vardhan, The ns nam manual, www.isi.edu/nsnam/ns/doc/index.html.

[14] Sergio Marti,T.J.Giuli, Kevin Lai and Mary Baker," Mitigating routing misbehaviour in Mobile ad-hoc networks". In Proceedings of MOBICOM 2000. Pages 255-256. 2000.

[15] H.Hallani and S.A.Shahrestani "Trust assessment in wireless Ad-hoc network"978-1-4244-2829,IEEE 2008.

[16] H.Hallani and S.A.Shahrestani, "Wireless Ad-hoc network : employing behaviour history to combat malicious nodes", In Proc. International Conf on Signal Processing and Telecommunication Systems(ICSPCS'07), Gold Coast , Australia, December, 2007, pp.1-6.

AUTHORS

Ananya Banerjee

She is associated with ECE department in Dr Sudhir Chandra Sur Degree Engineering College (WBUT) from 2010. She has started her carrier as a lecturer in Academy of Technology (WBUT) and then Institute of Engineering and Management (WBUT). In total 4.7 years experienced, Mrs. Banerjee has passed her M.Tech from Institute of Radio Physics and Electronics and M.Sc. in Electronic Science from University College of science and technology, Calcutta University. Having interest in Communication network, she has published one inter national journal paper on "Trust Improvement among the nodes in a Wireless Ad-hoc Network" International Journal of Advanced Research in Computer Engineering & Technology Vol. 1, Issue 3, May2012.

Sutanu Ghosh

Presently he is working as Assistant Professor in Electronics and Communication Engineering Department of Dr Sudhir Chandra Sur Degree Engineering College, Kolkata. After the completion of M.tech. Degree in Mobile Computing and Communication Engineering from Jadavpur University (2009), he is actively engaged in teaching since 2009. His current research interests are in the areas of Network Architecture and protocols, Integration Architecture of WLAN and 3G Networks,Voice Over IP network and Wireless Ad-hoc Networks. Mr. Ghosh is a Member of IAENG and IACSIT. He has published many research contributions in prestigious peer Reviewed journals.

Anirban Neogi

He is currently working as the HOD of ECE department of Dr. Sudhir Chandra Sur Degree Engineering College.She has started her carrier as a lecturer in Bengal Institute of Technology (Under Techno India Group). He has total experience of over 10 years in teaching. As a part of his research activity he got 6 international journal publications and few conference papers in the field of Nanoscience and as well as in Ad-hoc network. He did his M.Tech from Institute of Radio Physics and Electronics and M.Sc. in Electronic Science from university college of science and technology, Calcutta university.