ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 3, May2012

Trust Improvement among the nodes in a Wireless Ad-hoc Network

A.Neogi, A. Banerjee
Dr.Sudhir Chandra Sur Degree Engineering College, Kolkata-700074.

1. Abstract:
Ad-hoc network establish improvised communication with environment without any fixed infrastructure. Nodes in Ad-hoc network (MANET) do not rely on a central infrastructure but relay packets originated by other nodes. Mobile ad-hoc network can work properly only if the participating nodes collaborate with routing forwarding. Therefore it is required that the nodes co-operate for the intensity of operator network. Due to high mobility of the nodes in the network, detecting 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 and Efficient 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.

2. Introduction:
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. 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. 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 route 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 or AODV may not result the proper
routing. Enforcing the co-operation among the mobile nodes is particularly challenging which may solve for many routing issues.

3. Routing and security issues:

Co-operation and Fairness:
If the selfish node try to economised on their resources by not forwarding packets, total non collaboration with other nodes will result.

Location confidentiality:
The traceability of nodes, both the physical and logical location is a big issue. The node
identity is equally important as well as the message content.

No traffic Diversion:
Malicious nodes can attack unusual traffic to themselves by means of wrong routing information. They also can forward the information to their neighbours in wrong time sequence or in a collapsed format. The increasing numbers of such

malicious nodes will reduce down the efficiency of the network.

Attacks:
If the attackers use a non-optimal path that travels through the same nodes more than once is called Routing loops. A black hole attack is used by malicious node which makes all the traffic travel through routing loops and claims that it has the shortest routing path. The malicious nodes some times transmit incomplete information by dropping some selective packets, called gray hole attack. Another important issue is replay attack, where the attackers replay the already sent packets to the network.

4. DSR:
DSR is a reactive routing protocol for MANETs, proposed by Johnson & Mattz in order to provide routing with minimum overhead while adapting to the network dynamics. DSR operates on two simple and complementary mechanism , *i) route discovery and ii) route maintenance*. In DSR the source node puts the whole route in the data packets. Intermediate nodes belonging to this route do not use any data structure to store routing tables. Route discovery uses two types of control messages: i) the route request (RQ) and ii) the route reply(RP). The source node floods the network with RQ packets to reach the final destination node. On receiving this RQ packets an intermediate node checks whether it is the destination node or not. If it is true RP packet returns to source. If not, this node checks if it has already received a copy of the packet or if the accumulated header route of the RP is saturated. If true RP is dropped. Otherwise the intermediate node adds its own address in the RQ packet and rebroadcast the same message to all its direct neighbour. If no MAC acknowledgement is required, the upstream node declares the link as 'being broken'. In which case the node updates its cache and then sends a **Route Error Packet (REP)** to the source node.REP contains the broken link.

Such research work has been done to make the route discovered by DSR secure. The Watchdog and Pathrater mechanism has been specially designed to optimize the forwarding mechanism in the DSR. The Watchdog is responsible for detecting selfish nodes. The Pathrater
assigns different ratings to the nodes based upon the feedback that it receives from Watchdog. A trust based routing is proposed by Pirazada in which the trust agent derives trust levels from events that are directly experienced by a node. A reputation agent shares trust information 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.

The Trust Embedded AODV(T-AODV) was proposed to secure an ad-hoc network from independent malicious nodes by finding a secure end to end route. In this protocol trust values are distributed to the nodes a priori. In the route discovery phase the RQ packet header contains a trust_ level field in addition to the other fields. All the intermediate nodes rebroadcast the RQ after modifying the trust_ level by including the trust level of the node. The source node selects the route with highest value of the trust_ level matrices.

5. Proposed Scheme 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 a 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 a unknown node for the source node. This threshold value can be represented by a numerical value ie,0 .5.
This known node is classified into two categories i) Completely known and ii) Moderately known.
When Trust value of a known node is greater than 0.5 and less than .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.

Co-relation table:

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

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, *Td =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

Trustfield(new)=Trust field(previous)+Txy(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 Tf and for the reverse direction Trust field is denoted by Tr.

Total transaction:

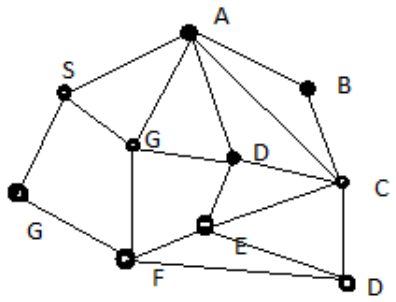

Fig 1 : A Network

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 neighbour

nodes with Tf 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-A-B-C-D 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:

Tf(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 a 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:

Tr(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

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

Where, $Si=1/xi/\sum_{i=1}^{x} 1/xi$, for ith possible path

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

6. Performance Analysis:

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.

7. Result:
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.

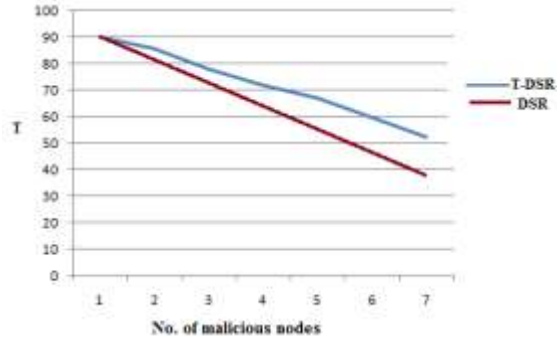

Fig:R1

In figR1 the achieved throughput is clearly greater than the standard DSR.

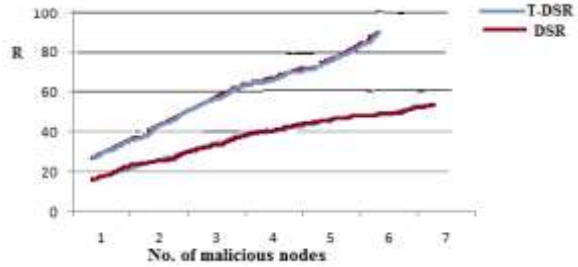

Fig: R2

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

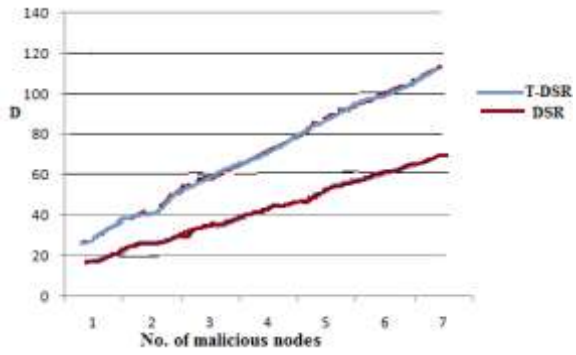

Fig: R3

Fig: R3 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.

8. Conclusion and Future work:

In this paper we have discussed the characteristics of mobile ad-hoc network, we also analyze the different types of security issues and attacks to the network. The proposed Trust Enhancement scheme enhance the level of security routing and also force the nodes to co-operate in 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.

9. References:

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

[2]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.

[3] Huaizhi Li, Mukesh Singha, *"Trust Management in Distributed Systems"* IEEE Computer Society February 2007.

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

[5] 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.

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

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

[8] 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 , www.tml.tkk.fi/Publications/C/22/papers/Jimenez_final.pdf

[9] 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.

[10] 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.

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

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

[13] 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.