2-Tier Trust Based Model Forintrusion Detection System in Mobile Adhoc Network

Suchita B. Patel, Dr. Samratvivekanand O Khanna

[1]*Ph.D. Student, S. P. University, Assistant Professor, ISTAR College, V.V.Nagar, Gujarat, India*

[2]*Professor & Head, MSc(IT) Dept., ISTAR College, V.V Nagar, Gujarat, India*

Abstract: **Mobile Adhoc Networks (MANET) is a set of wireless cellular nodes which creates transient network with none infrastructure. The channel is wi-fi, topology is dynamic so, there may be no clear line of defense. due to those motives, MANET constantly stays under extra danger to attacks. The Black hole assault is considered one of such safety issue in MANET. In a Black hole assault a malicious node replies with having a shortest path to destination and drops the send packet by way of supply node in preference to forwarding it to the vacation spot node. on this paper, we propose 2-tier trust based model to preventattacks by using calculating believe cost for source to destination in between hops as well as consider for course and store facts for routing motive. by using depended on routing protocol named 2-tier NTPTSAODV (Node accept as true with course accept as true with comfy AODV) affords at ease network transmission direction. The NTPTSAODV protocol has been implemented and simulated on NS-2. The overall performance of NTPTSAODV has been additionally analyzed with appreciate to Blackhole attack and examine with normal AODV, BAODV and NTPTSAODV.**

***Keywords*-Node Trust, Path Trust, Secure AODV, MANET-Mobile Adhoc Network, Trust, Malicious.**

I. INTRODUCTION

An Ad Hoc Network[1] is a collection of Wi-Fi nodes which have the capacity to talk with every different without having fixed community infrastructure or any imperative base station. seeing that nodes are not controlled via every other controlling entity, they have unrestricted connectivity to others. Routing and community control are completed cooperatively by way of each different node because of constrained transmission power, multi hop structure is needed for one node to speak with every other thru community. in this multi hop structure, every node works as a host and as well as a router that forwards packets for other nodes that may not be inside a right away communication variety. each node participates in an ad hoc course discovery protocol which finds out multi hop routes thru the network among any nodes. These infrastructures-much lessnodes in ad hoc networks dynamically create routes amongst themselves to shape personal wireless community on the fly.

Thus adhoc networks offer an incredibly flexible verbal exchange method for any region in which geographical or terrestrial constraints are gift and any constant structure, along with battlefields, and a few catastrophe control conditions. The AODV (adhoc on call for distance vector routing) [5]protocol is prone to the well-known black hole attack. A black hole is a node that always responds definitely with a RREP (Request reply) message to each RREQ (course Request), even though itdoes now not surely have a valid path to the vacation spot node. because a black hole node does not have to test its routing desk, it's miles the first to respond to the RREQ in most instances. Then the supply routes records thru the black hole node,that allows you to drop all the records packets it received as opposed to forwarding them to the destination. in this way the malicious node can without difficulty misroute lot of community site visitors to itself and could motive an attack to the community with verylittle attempt on it. those black hole nodes may go as a group. meaning a couple of black hole nodes work cooperatively to deceive other nodes [7]. This kind of attack is called cooperative black hole attacks which harm the networks performance severely.

1.1 Blackhole Attacks:

Malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will at once ship a fake RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the sparkling route in the direction of the destination. The source node ignores the RREP packet obtained from other nodes and starts sending statistics packets to malicious node. A malicious node takes all the routescloser to itself. It does no longer permit forwarding any packet everywhere. This attack is called a Black hole because it swallows all the records packets.

on this paper we propose 2-tier consider version within the Adhoc On Demand for Distance Vector (AODV) routing protocol calls - NTPTSAODV (Node accept as true with direction trust secure AODV) protocol that consist of calculation of trust for first Neighboring Node and then Routing Path. NTPTSAODV can lessen the threat on MANET that because of black hole attacks. It additionally will increase the packet delivery fraction by means of selection the excellent route.

II. RELATED WORK

[1] Piyush et.el[6] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If checking fails, then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers this solution becomes vulnerable.

[2] Payal et.al [2] suggested a protocol DPRAODV that finds a threshold value and compares that with difference of sequence number of reply packet and that of route table entry. If it is higher than the threshold value, the node sending reply is added to a list of blacklisted nodes. Also an ALARAM packet containing blacklisted node is sent to its neighbors to inform that reply packets from the malicious node are to be discarded. The protocol has higher routing overhead due to addition of the ALARAM packets.

[3] A trust based approach is proposed by Arshad et.al[8] that uses passive acknowledgement as it is simplest; it uses promiscuous mode to observe the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for. Thus, a node can make sure that packets it has sent to the neighboring node for forwarding are indeed forwarded. Routing choices are made based on two parameters: Trust and hop-count; therefore, the selected next hop gives the shortest trusted path. Though, monitoring overall traffic would have been a better choice instead of monitoring one node's request.

[4] TAODV [9] is another protocol based on trust which calculates it on the basis of others opinion. This method uses two additional special messages: Trust Request (TREQ) and Trust Reply (TREP) and adds addition 3 new fields to the routing table for calculating the trustworthiness of nodes. TAODV use digital signature which is an additional overhead. Opinion of other nodes cannot be trusted as it can also be from malicious nodes itself. This is an extension of basic AODV protocol.

[5] A Balaji Proposes a trust based approach [10]using AODV protocol. But they do not consider the data packets. Insteadthey consider only control packets like RREQ, RRER and RREP and network layer acknowledgement. A black hole caneven drop data packets by perfectly transmitting control packets. There the system fails by thinking there is no blackhole as the control packets are transmitted without any delay or drop.

III. PROBLEM IDENTIFICATION

A study of the existing works helped us in identifying the following main problems:

i) Many of the solutions proposed in existing works can detect and prevent single black-hole attack but cannot prevent a cooperative black hole attack.
ii) Many solutions neglected increase in average end to end delay and
iii) routing overhead.
iv) Mobility of nodes is another important concern in case of mobile environment.

IV. PROPOSED 2- Tier TRUST MODEL, NTPTSAODV ROUTING PROTOCOL

Many trust primarily based methods have been proposed to evaluate agree with values for simplest manipulate packets based totally on node conduct at community Layer. The concept of accept as true with at first derives from social sciences and is described because the degree of subjective belief about the behaviors of a specific entity.

4.1 Solutions Proposed:

Proposed solution aims to serve the following purposes:

[1]. To detect the Blackhole attacking node/s
[2]. To determine the most trustworthy nodes for secure data packets transmission.
[3]. To determine most suitable trustworthy paths/routes between source to destination

Our goals of proposed schemes are to measurement of trust can be application dependent where trust can be represented by Quantitative Value.The node trust and path trust plays a very crucial role in MANET routing. Trust factor here focuses onidentifying the nodes which not suitable for reliable routing and helps to select best path to carry on routing successfully using reliable nodes.

The proposed work concentrates onidentifying these unreliable nodes using the trust level values calculated for each node.The architecture of proposed NTPTSAODV routing protocol with 2-Tier Trust Model is presented in Figure-1.Trust model essentially performs trust derivation and computation.

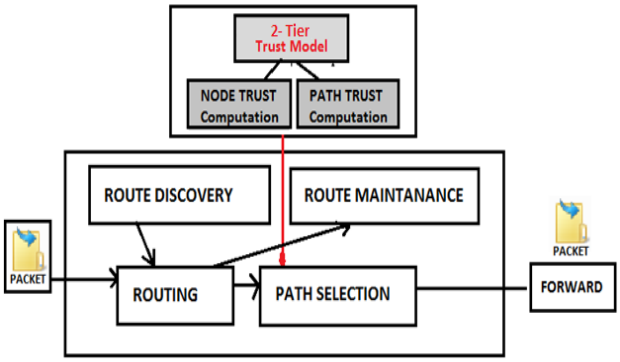

Figure 1: An Architecture of proposed NTPTSAODV routing protocol with 2-Tier Trust based Model

We know, in MANET, the network topology changes dynamically. But, this fact has not been considered in many of the existing solutions.

2-Tier Trust Model of NTPTSAODV is implemented by computation of Node Trust (NT) and Path Trust (PT) to secure AODV routing protocol.

The proposed work focuses on each node will maintain a trust value for every one-hop neighbor to which packets have been sent for forwarding.We also consider mobility of the nodes factors in the network and then propose our solution.

4.2 Computation on Node Trust (NT):

In computation of Node Trust (NT) we propose a Quantitative Numeric Value approach for detecting trustworthy nodes using the trust level values calculated for each node.

According to our proposal, computation of node trust in network is based on parameters such as stability of node defined by its mobility and pause time, control packets and data packets etc.

This trust of nodes provides selection of most reliable trustworthy route for data transmission. In mobile ad hoc networks, all packets can be classified into two types:

- control packets and
- data packets

The trust level value calculation is based on the parameters shown in the table **[A]**The Actual Node Trust (NT) calculation can be divided into two parts:

*4.2.1 Trust Calculation from Control Packets (**TCP**):*

It shows how the trust will be affected by the routing information on the given node.

*4.2.2 Trust Calculation from Data Packets (**TDP**):*

It shows how the data transmission can affect trust on the given node.

Table 1: Node Trust computation parameters

COUNT TYPE	RECEIVED At Node	Total RECEIVED from each Node
RREQ	Rrreq	Rrreqt
RREP	Rrrep	Rrrept
RERR	Rrerr	Rrerrt
DATA PACKET	Dpr	Dps
NODE STABILTIY	**VELOCITY**	**PAUSE TIME**

Here **COUNT TYPE** describes success and failure rate which describes whether the packet transmission was a successful or unsuccessful transmission.

RREQ ,**RREP, RERR** are the route request, route reply and route errorare control packets respectively which are exchanged between nodes in the network.

DATA PACKET refers to the pay load transmitted by the node in the routing path.

From these two sub- calculations we get the final value of Trust, which is stored in each node in structure. Analysis of individual fragment values are given in equation (1), (2), (3), (4) and (5)

$$F1 = \left\lceil \frac{1}{\mathbf{Min(RREQ,\ RREQ\_T)}} \right\rceil * \left\lceil \frac{(\mathbf{RREQ - RREQ\_T})\ 2}{(\mathbf{RREQ + RREQ\_T})} \right\rceil \quad \ldots\ldots (1)$$

$$F2 = \left\lceil \frac{1}{\mathbf{Min(RREP,\ RREP\_T)}} \right\rceil * \left\lceil \frac{(\mathbf{RREP - RREP\_T})\ 2}{(\mathbf{RREP + RREP\_T})} \right\rceil \quad \ldots\ldots (2)$$

$$F3 = \left\lceil \frac{1}{\mathbf{Min(RRERR,\ RRERR\_T)}} \right\rceil * \left\lceil \frac{(\mathbf{RRERR - RRERR\_T})\ 2}{(\mathbf{RRERR + RRERR\_T})} \right\rceil \quad \ldots\ldots (3)$$

$$F4 = \left\lceil \frac{1}{\mathbf{Min(DATA,\ DATA\_T)}} \right\rceil * \left\lceil \frac{(\mathbf{DATA - DATA\_T})\ 2}{(\mathbf{DATA + DATA\_T})} \right\rceil \quad \ldots\ldots (4)$$

Furthermore, values **RREQ, RREP, RRERR**and **DATA** represents specific values of specific packets received from a given node and **RREQ_T, RREP_T, RRERR_T** and **DATA_T** are the values of total number of packets received on the given node.

Where **F1, F2, F3** and **F4** are Final values that are used to calculate the nodes Route Request rate, RouteReply rate, Route Error rate and data packet transmission rate.

The derived trust is denoted by T(cp) and T(dp).**W1, W2, W3, W4** are constants, which defines a weight of trust value. Constant can be changed based on types of attack and basis of what we want to balance with the individual parameters entering into calculation of trust.

W1 = [(Rrreq - Rrreqt) / Min(Rrreq, Rrreqt)]

W2 = [(Rrrep + Rrrept) / Min(Rrrep, Rrrept)]

W3 = [(Rrerr + Rrerrt) / Min(Rrerr, Rrerrt)]

W4 = [(Dpr + Dprt) / Min(Dpr, Dprt)]

CONTROL PACKET FACTOR:

$$T(cp) = W1 * F1 + W2 * F2 + W3 * F3 \quad \text{.....(5)}$$

DATA PACKET FACTOR:

$$T(dp) = W4 * F4 \quad \text{.....(6)}$$

4.2.3 Node Stability Factor:

This parameter represents the stability of a node. higher the cost of this parameter manner more solid node. we've considered the Random Waypoint version in figuring out the mobility of the nodes inside the community.

the two parameters in this model are the pause time (Tpause) and maximum allowable velocity for every mobile node (maxV). in keeping with this model, every cell node randomly selects a area as its destination. It then travels towards this vacation spot with consistent velocity chosen uniformly and randomly from [0, maxV]. Upon attaining the destination, the node stops for a period described through the 'pause time' parameter (Tpause).

If the relative pace of a node w.r.t the source node is low and the pause time is long, the topology of the network becomes exceedingly solid. then again, if its relative speed is high and the pause time is low, the topology becomes highly dynamic. In the course of the route discovery procedure and packet sending by means of source node, an inexpensive time is taken; if the node decided on for forwarding the packets has excessive relative pace w.r.t source node, then by the time packets are dispatched to it, this node won't be in the identical function as earlier than. So, if it isn't always in its preceding position, then it'll now not be able to ahead the packets; the topology adjustments and subsequently once more the route discovery method has to be initiated. therefore, a node which is less cellular w.r.t to the source node is extra premiere for packet forwarding.

Node Stability is calculated as following:

NS = Tpause / Vnode ..... (7)

[where**Vnode** is the relative velocity of the node w.r.t to the source node and **(0≤ Vnode ≤ Vmax).**]

The Value representing Final Node Trust we combine these three factors of a node into a singleone and we call it as trust factor of a node as follows shown in equation……..(8)

ANT (Average Node Trust) = T(cp) * T(dp) * NS …. (8)

Thus, each node in the network has a value of trust. We may say that greater the value of trust of a node, the more suitableor reliable it is for packet transmission.

4.3 Computation of Path Trust

The source node wants to send packets to destination node it initiates route discovery. After route discovery is complete source node finds there are three routes available for transmitting packets to destination node. Now it has to decide which route to select. Proposed algorithm is applied after route discovery phase.When a source discovers a path to the destination with the help of forwarding nodes, the trust value of path should be computed according to the trust values of nodes.

Table 2: Parameters of Nodes in MANET

Node ID	RREQ		RREP		RERR		DATA PACKET		NODE STABILTIY		
	Received	Total	Received	Total	Received	Total	Received	Sent	VELOCITY	PAUSE TIME	NS = V/P
1	128	234	87	147	12	25	2467	1447	30	10	0.33333
2	475	268	24	88	13	29	2674	4325	40	10	0.25
3	120	200	98	200	8	21	3243	4532	10	10	1
4	324	120	87	147	22	12	4325	4500	30	10	0.33333
5	456	324	24	88	10	21	2321	1299	20	10	0.5
6	135	245	87	147	30	12	2453	3423	20	10	0.5
7	245	200	24	88	10	21	3212	2132	30	10	0.33333
8	432	414	87	147	13	24	4321	2431	20	10	0.5

Table 3: Parameters of Nodes in MANET for trust calculation

Node ID	CONTROL PACKET TRUST FACTOR PARAMETERS			CONTROL PACKET TRUST FACTOR – T(cp)	DATA PACKET TRUST FACTOR - T(dp)	NODE STABILTIY FACTOR- (NS)
	FRREQ	FRREP	FRERR	= (FRREQ) * 1! + (FRREP) * 2! + (FRERR) * 3!	FDP	
1	0.54700855	0.59183673	0.48	4.61068202	1.7049067	0.33333
2	1.77238806	0.27272727	0.448276	5.00749778	0.6182659	0.25
3	0.6	0.49	0.380952	3.86571429	0.71557811	1
4	2.7	0.59183673	1.833333	14.8836735	0.96111111	0.33333
5	1.40740741	0.27272727	0.47619	4.81000481	1.78675905	0.5
6	0.55102041	0.59183673	2.5	16.7346939	0.71662285	0.5
7	1.225	0.27272727	0.47619	4.6275974	1.5065666	0.33333
8	1.04347826	0.59183673	0.541667	5.47715173	1.77745784	0.5

If between source node to destination node, there are three following routes available,

Route-1: 1-2
Route-2: 3- 4-5
Route -3: 6-7-8

Average Route Trust = Avg. T(cp) * Avg. T(dp) * Avg. NS……..(9)

Table 4: Average Parameter Values

Route	Avg. T(cp)	Avg. T(dp)	Avg. NS	Avg. Route Trust
1	4.8090	1.1615	0.2916	1.6292
2	**7.8531**	**1.1544**	**0.6111**	**5.5405**
3	8.9464	1.3335	0.4444	5.3024

First all nodes trust value calculates in (table-2) using equations (5), (6), (7) and then calculates Average trust for routes using equation (8). Thus average trust values for routes are given in Table-3. Finally, **route 2 will be selected for transmitting path for packets because it has a highest trust value among three routes.**

TRANSMITION PATH: (TP) = AVERAGE HIGHEST TRUSTED ROUTE VALUE.

Thus each node and subsequently each path will be selected for transmission only after considering all these parameters. This would ensure trusted transmission path of packets and at the same time secure route utilization as well.

V. CONCLUSIONS AND FUTURE WORK

This Transmission path selection value is used to select most trusted route rather than selecting shortest or longest path. This significantlyimproves the trust factor on the neighboring nodes in the network.Thus we conclude that the trust based 2 – Tier NTPTSAODV routing protocol proposed in this paper improves the security level and also prevent malicious node attack in the network. In future we are going to implement our own performance evaluation tool which gives us comparative result analysis of all three normal AODV, Black Hole AODV(BAODV) and NTPTSAODV routing protocols.

REFERENCES

[1]. C.E. Perkins, S,R, Das, and E. Royer: "Ad-I-Ioe on Demand Distance Vector(AODV)", RFC 3561.
[2]. Payal N. Raj and Prashant B. Swadas, "DPRAODV: A Dynamic Learning System Against Black Hole Attack InAODV Based Manet", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[3]. Z. Li, A. Das, J. Zhou; "Theoretical Basis for Intrusion Detection"; Proceedings of 6th IEEE Information Assurance Workshop (IAW), 2005

[4]. JENSEN C.D., CONNELL P.O.: 'Trust-based route selection in dynamic source routing'. Proc. Int. Conf. on TrustManagement, Pisa, Italy, May 2006, pp. 150–163

[5]. H. Xia, Z. Jia, X. Li, L. Ju and E.H.M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks, 2012, Available online 25 February 2012,http://dx.doi.org/10.1016/j.adhoc.2012.02.009.

[6]. Suchita B. Patel, "Blackhole Attack Putting into Practice in AODV Routing Protocol", International Journal of Mobile & Adhoc Network|Vol 4|issue 4|Nov. 2014, pp. 352-355.

[7]. Suchita B. Patel, Dr. Samrat O. Khanna, "Black Hole Attack Detection Solutions Using AODV Protocol for MANET: A Review" International Journal of Computer Networks and Security, ISSN:2051-6878, Vol.24, Issue.1, RECENT SCIENCE PUBLICATIONS ARCHIVES |April 2014|$25.00 | 27703429| PP. 1224-1233.

[8]. Asad Amir Pirzada and Chris McDonald. Establishing Trust InPure Ad-hoc Networks. In Proceddings 27th AustralasianComputer Science Conference (ACSC'04), Dunedin, New Zealand,26(1), pages 47-54, January 2004.

[9]. A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks.PhD thesis, Department of Computer Science and Engineering,The Chinese University of Hong Kong, 2003.

[10]. N. Bhalaji, A. Shanmugam, "A Trust Based Model to MitigateBlack Hole Attacks in DSR Based Manet", European Journal ofScientific Research, ISSN 1450-216X Vol.50 No.1,2011.