Trustbased Multipath Routing technique for blackhole detection and prevention in MANET

Jyoti Agarwal
Dept. of Computer Science & Information Technology
Madhav Institute Of Technology & Science
Gwalior (M.P)

Neha Bhardwaj
Dept. of Computer Science & Information Technology
Madhav Institute Of Technology & Science
Gwalior (M.P)

Abstract—**Most of the techniques that are used to mitigate blackhole attack are based on the use of destination sequence number as a criterion to identify blackhole node. However, these schemes have limitation of quantifying the value of destination sequence number that is used to identify a black hole node. In this paper we present an AODV based mechanism to avoid malicious node (i.e.blackhole attack). In proposed scheme, the trust based multipath routing algorithm is used for finding the misbehaved node. Through trust based approach trust is to be calculated and trusted path is chosen among multipath network. We have simulated the scenario by using NS 2.35 using TCL and C language. Our schemes prove the dominance over preliminaries in terms of packet delivery ratio and throughput.**

Keywords—Mobile Adhoc Network,AODV, Attacks in MANET,Blackhole Attack.

I. INTRODUCTION

MANET is a self-designing system of mobile nodes that are connected in remote environment. All the devices in a MANET are free to move in any direction, as a result links between the devices change frequently. Every nodeforward packet to all neighboring nodes within the range that isn't intended for its own utilization and in this way it goes till the destination. So what packet drop attack or blackhole attack simply occurs; it is basically the act of dropping the packet instead of forwarding them, by a malicious node. In MANET routing protocols are categories into two classes proactive routing and reactive routing [1].

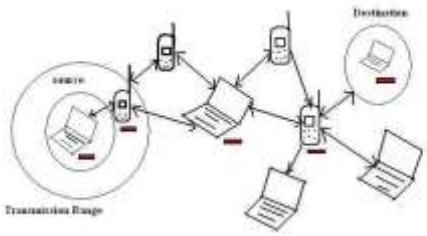

Fig. 1: MANET

Routing protocols in MANETs is the adhoc ondemand distance vector (AODV) routing convention. It is a source started on-request directing convention. Be that as it may, AODV is helpless against the outstanding blackhole attack. During blackhole attack, a malicious node catches bundles and not advances them in the system and publicizes itself as having the shortest way to the node whose parcels it needs to capture in the event that in excess of one malignant node cooperate as a gathering then the harm will be intense. This sort of attack is called cooperative black hole attack[2].

II. COUNTER MEASURES FOR MANET SECURITY ATTACKS

Successful deployment of MANET in variety of applications depends on the level of security services. A security administration can be characterized as a preparing or correspondence benefit that is given by a framework to give a particular sort of assurance to framework assets. This section [3] analyses variety of solutions proposed to defend the attacks.

Physical Layer assaults can be guarded by Spread spectrum technology, for example, frequency hopping (FHSS) or direct sequence (DSSS), which can make it hard to distinguish or stick signals. It changes frequency in a random fashion to make signal capture difficult or spreads the energy to a wider spectrum so the transmission power is hidden behind the noise level.

Data Link layer attacks can be safeguarded by plans, for example, ERA-802.11, where identification calculations are proposed. Traffic analysis is prevented by encryption at information connect layer. The Wired Equivalent Privacy (WEP) encryption conspire characterized in the IEEE 802.11 remote LAN standard uses connect encryption to conceal the conclusion to-end movement stream data. Another approach is to create a security cloud, construct a traffic cover mode or dynamic mix method, or use traditional traffic padding and traffic rerouting techniques to prevent traffic analysis.

Transport Layer: Secure Socket Layer (SSL), Transport Layer Security (TLS), and Private Communications Transport (PCT) conventions were intended for secure interchanges and depend on open key cryptography. TLS/SSL must be adjusted keeping in mind the end goal to address the uncommon needs of MANET.Some firewall configured to defend against SYN flooding attacks.

Application Layer firewalls can effectively prevent many attacks, and application-specific modules. However, a firewall is mostly restricted to basic access control and is not able to solve all security problems and hence, an Intrusion Detection System (IDS) can be used as a second line of defense.

- **Network Layer**

1) **Wormhole Attacks:** A packet leash protocol is designed as a countermeasure to the wormhole attack. The SECTOR instrument is proposed to perceive wormholes without the need of clock

synchronization. Directional gathering devices are similarly proposed to avoid wormhole attacks.

2) **Blackhole Attacks:** Some routing protocols, for instance, security-aware ad hoc routing protocol, can be utilize to protect beside blackhole attacks. ARAN constrains or averts assaults that can influence other insecure protocols.Multiple node attacks against MANET are ordered as immediate direct collaborative attacks and indirect collaborative attacks. Blackhole and Wormhole attacks have a place with direct collaborative attacks class.

3) **Impersonation and Repudiation Attacks:** ARAN can be utilized to protect against pantomime and disavowal assaults. It gives verification and non-renouncement administrations utilizing foreordained cryptographic declarations.

III. BLACKHOLE ATTACK IN AODV

In a blackhole attack [4], a malicious node can imitate a goal node by sending a ridiculed route packet to a source node that starts a route revelation. A blackhole have two properties:

- The node abuses the ad hoc routing protocol, for example, AODV, to publicize itself as having a legitimate course to a goal, despite the fact that the course is deceptive, with the expectation of catching packets.
- The node devours the captured packets. In an ad hoc network that uses the AODV convention, a blackhole node ingests the system activity and drops all packets. To clarify the blackhole assault we include a malevolent node that displays blackhole conduct in the Fig. 2.

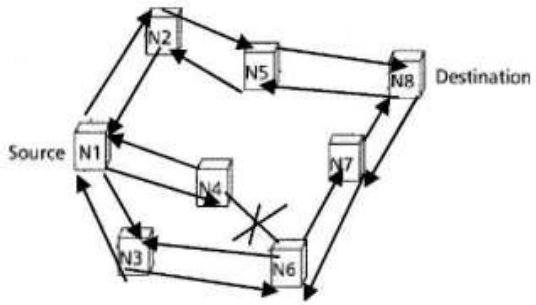

Fig. 2: Blackhole in AODV

In Fig. 2, we accept that node N4 is the malignantnode. Assume node N1 needs to send information bundles to node N8 in Fig. 2, and starts the course disclosure process. We accepted node N4 is a malicious node with no fresh enough course to goal node N8. Be that as it may, node N4 claims that it has the course to the goal at whatever point it gets RREQ packets, and sends the reaction to source node N1. The destination node and any other normal intermediate nodes that have the new course to the goal may likewise give an answer. If the appropriate response from a customary center accomplishes the source center of the RREQ. Initially, everything functions admirably; yet the answer from malicious node N4 could achieve the source node first, if the malicious node is closer to the source node. Also, a malignant node does not need to check its directing table when sending a false message; its response will most likely accomplish the source node first. This makes the source node feel that the course revelation process is finished, overlook all other answer messages, and start to send data packets. Accordingly, every one of the packets through the malicious node are basically overwhelmed or lost. The malicious node could be said to shape a black hole in the system. Along these lines the malicious node can without much of a stretch misroute a great deal of system movement to itself, and could make an assault the system with next to no endeavors on its part.

IV. LITERATURE SURVEY

Nikhil G. Wakode[2017] This paper is used to solve malicious nodes by using Ad hoc demand distance vector (AODV) routing by cooperative bait detection approach (CBDA) with Pernicious node identification calculation. The CBDA escaped responsive and proactive routing mechanism. Malicious node recognition calculation identifies the malicious node in the system. It actualizes an invert following way to deal with accomplish the coveted objective. Simulation results have specified, AODV, presence of malevolent node in AODV and securing malicious nodes in AODV by utilizing CBDA with Malicious node recognition calculation as far as packet delivery ratio, end-to-end delay, normalized routing overhead and packet dropped ratio (taken as execution lattices) [6].

Kamel et al. [2017] a secure and trust based approach based on ad hoc on demand distance vector (STAODV) has been projected to improve the security of AODV directing convention. The methodology secludes the malignant nodes that endeavor to assault the system relying upon their past data. A trust level is joined to each taking an interest node to identify the level of trust of that node. Every approaching bundle will be analyzed to keep the black hole attack [6].

Pradeep R. Dumne and AratiManjaramkar[2016] proposed a technique to determine this issue by utilizing malignant node discovery pattern in light of DSR instrument - cooperative bait detection scheme (CBDS) which utilizes hybrid protection models. CBDS system discovers vindictive node by utilizing a switch following strategy. The essential and proposed CBDS plans are actualized in NS-2.35. Results are analyzed based on throughput, PDR [7].

Mohamed A. Abdelshafy and Peter J. B. King [2016] present a Blackhole Resisting Mechanism (BRM) to oppose such assaults that can be fused into any reactive routing protocol. It doesn't require costly cryptography or verification components, yet depends on privately connected clocks and limits to order nodes as vindictive. No alterations to the bundle groups are required, so the overhead is a little measure of estimation at nodes, and no additional correspondence. Using NS2 simulation, we compare the performance of networks using AODV under blackhole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a blackhole attack [8].

NeerajAryaet al [2015] This paper incite to recognize and avoided of worm hole attack and collaborative black hole attack using trusted AODV routing algorithm [9].

KritiPatidar and VandanaDubey [2014] presents an IDSin view of the idea of determination based identification framework to identify and counteract blackhole attacks. This paper likewise shows a hop count examination way to deal with recognize wormhole attacks along courses in impromptu systems. The proposed convention does not require any area data, time synchronization, or uncommon equipment to recognize wormhole attacks. The protocols are evaluated using analysis and simulations on network simulator [10].

Ms Monika Y. Dangore and MrSantosh [2013] here, the impact of blackhole attacks in AODV based system is contemplated. The framework parameters like Throughput, Packet Delivery Ratio and Average End to End Delay are figured for common framework (without blackhole) and a framework with one blackhole. In the wake of recognizing the blackhole assault remembering the true objective to proceed with data transmission, the blackhole node is dodging and the route to the real goal is continued once more. The execution of system parameters are thought about in all the three situations [11].

Rutvij H. Jhaveri et al. [2012] propose a plan for AODV protocol, in which a middle of the node distinguishes the malevolent node sending false routing information; routing packets are utilized not exclusively to pass directing data, yet in addition to pass data about noxious nodes. The proposed plot recognizes as well as expels malignant node by disengaging it, to make protected and secure correspondence [12].

SiddharthDhama et al [2016] proposing a mechanism for the detection and preventionof BH attack in the mobile ad hoc network. The routing protocolthat we are using is Ad hoc on-demand distance vector routing(AODV). As we know that AODV is vulnerable to BH attack,where a node pretends as a shortest path node and gives falseinformation to the sender. In this paper we not only preventingbut also detecting the BH node. The simulator used here toimplement the mechanism is NS 2 and result proved theeffectiveness of model as the throughput is very high ascompared to AODV that does not have proposed mechanism.[14]

Base algorithm for the detection of BH attack

Notations:
SN: Source_node
DN: Destination_node
IN: Intermediate_node
RREQ: Route_request
RREP: Route_reply
SN: Sequence_number
HC: Hop count
RT: Routing table
Store Entry: denotes the routing table entry for storing RREP_Entry.
New_RREP_tab: denotes the new routing table for storing routing table entry.
Step: 1- // when source node got RREP packet from malicious blackhole node //
RREP_recvReply (packet_p)
{
Rrep Header RREP_Entry;
P_> remove header (RREP_Entry)
Get_Sq N = recv_RREP_Sq N
Step: 2- // Science Sq N in RREP has its maximum limit (which is 32 bit unsigned value 4294967295) //
while (RREP_Sq N < = max.(u_int32))
{
Do ("Sq N reset to zero");
}
Step: 3- // Store new RREP tab entry //
New_RREP_tab.add(store_entry);
Step: 4- // If the substraction result of the Sq Ns, currently stored in a node, and Sq N Of incoming AODV_RREP_P is less than zero (i. e negative). Confirm it that The node is attacker //
If ((dst_Sq N store_entry – rt_src_Sq N) < = 0))
{
Do ("node is attacker");
New_RREP_tab delete route (dst_Sq N store_entry)
}
Step: 5- End

V. PROPOSED METHODOLOGY

A. *ProblemStatement*

If the subtraction result of the Sq Ns, currentlystored in a node, and Sq N Of incomingAODV_RREP_P is less than zero (i. e negative).Confirm it that The node is attacker // but sometime this technique fail to detect if hacker node replies with correct sqnumber . To overcome this problem we have proposed a multipath trust based entrance to get better security.

B. *Proposed Methodology*

This research has focused on providingsolution for the black hole problem by enhancingmultipath algorithm resulting in regaining of theaverage no. of hops by not including the attacker nodes. Study has started with building a MANET in NS2 simulator with Random Waypointmobility Model for providing mobility with AODVas routing protocol.

In MANET, every one of the nodes in the systems isequity and capacities as terminal too router.There is distinction in execution rather offunction. The primary preferred standpoint of the structure is that there are various ways between source destination pairs. So it can circulate activity into multiple ways, diminish clog and eliminate conceivable "bottleneck". Be that as it may, MANET with the plane structure will increment routing control overhead; the adaptability issue is likely to occur.

- Utilizing grouping calculation to construct hierarchical topology might be a decent strategy to solve these issues. A versatile portable cluster algorithm can maintains the portability skillfully and maintains the security and strength of system design.

- To support the multi hop and mobilecharacteristics of wireless ad hoc network, therapid deployment of network and dynamicreconstruction after topology changes areeffectively implemented by clusteringmanagement.

Clustering management has five exceptional points of interest over different conventions.First, it uses multiple channels effectively andimproves system capacity greatly. Second, itreduces the exchange overhead of controlmessages and strengthens node management.Third, it is anything but

difficult to execute the nearby synchronization of system. Fourth, it providesQOS for variedmediumreimbursementcompetently. At last, it can support the remote systems with an extensive number of nodes.

C. How to Trust is Calculated

In [13] trust is deliberated as number of packets lost upon packets sent. It is achieved in indiscriminate mode (i.enodes keeps listening to its neighboring nodes).It keeps track ofnumber of data packets forwarded and dropped by therespective node. This would help to calculate the trustvalues for neighbor nodes.Each and every nodes trust values are taken to be inthe range of [0,1]. A trust numeric of 1 indicates acomplete trust, a node with a numeric of 0.5 indicatesignorance and a trust value of 0 signifies distrust. Nowtrust value of a node j calculated by a node i at aparticular time t is represented as $T_{ij}(t)$. It additionally considersthe weighted normal of soundness, unselfishness,connectivity, and vitality.

This paper gives a thought for straight and roundabout calculations of trust esteems for nodes. In direct trust computation, each node observes the events of itsneighbor node and reports to the 'knowledge' cache. Thetrust or will make a comparison of the report with its ownobservation report. With this as a factor, trust iscomputed. It considers four factors viz. route replymisbehavior, route request misbehavior, route errormisbehavior and data delivery misbehavior.In recommendation based trust computation, trustcomputation is established on voting. The trust valueshave a confidence of c ranging from [+1,-1]. If c has avalue of +1, it indicates completely positive confidence; -1 for completely negative confidence and 0 signifiestotally uncertain.

Since trust computations considers both success ratesand failure rates of data transmitted, uses cumulativesum of events. It is given with Cs represent the increasingsum of winning events of a category and Cf is theincreasing sum of failed events of a category. By thisway, the values are recorded and then normalize. Thisnormalized value falls into the range of -1 and +1. Ifthere exists more failures then may result in negativetrust value. Value of 0 signifies non- causal event andpositive value for supreme trust. Finally trust on node xby node y is calculated. The direct trust includesparameters like Packet Acknowledgments and Packet Precision.

To stay away from the blackhole attack, proposed algorithm has been executed in situation affected by blackhole assaults and this endeavored to standardize the scenario to its unique state.

D. Proposed Algorithm

SN: Source_node
DN: Destination_node
IN: Intermediate_node
RREQ: Route_request
RREP: Route_reply
SN: Sequence_number
HC: Hop count
RT: Routing table
Store Entry: denotes the routing table entry for storing RREP_Entry.
New_RREP_tab: denotes the new routing table for storing routing table entry.
Rnode: Random node
Avg_wt : Average waiting time
M: Malicious node
NT: Node trust
PT: Path trust
Avg_DN: Average destination
Avg_wt: Average waiting
Wt_DN : Waiting destination node

Step: 1- // when source node got RREP packet from Maliciousblackhole node //
RREP_recvReply (packet_p)
{
Rrep Header RREP_Entry;
P_> remove header (RREP_Entry)
Get_Sq N = recv_RREP_Sq N
Step: 2- // Science Sq N in RREP has its maximum limit (which is 32 bit unsigned value 4294967295) //
while (RREP_Sq N < = max.(u_int32))
{
Do ("Sq N reset to zero");
}
Step: 3- // Store new RREP tab entry //
New_RREP_tab.add(store_entry);
Step: 4- // If the subtraction result of the Sq Ns, currently stored in a node, and Sq N Of incoming AODV_RREP_P is less than zero (i. e negative).
Confirm it that
The node is attacker //
If ((dst_Sq N store_entry – rt_src_Sq N) < = 0))
{
Do ("node is attacker");
New_RREP_tab delete route (dst_Sq N store_entry)
}
Step: 5-Rnode = Rand(0 to max no of node)
Generate RREQ(Rnode)
// Wait for Response
Receive RREP(Rnode)
Step : 6- For a destination DN
Generate RREQ(DN)
Receive RREP(DN)
Calculate HC
Calculate Delay
Calculate Avg_wt
Step : 7- if((HC_DN<<Avg_DN)//(Wt_DN<<Avg_wt))
Than mark route as suspicious
Step :8- Request for neighboring information and find suspicious information
Select top suspicious
Find common node M1,M2…….Mn
Step :9 Delete suspicious route and mark M1,M2….Mn malicious node
Step : 10- Trust information
NT =No. of packets dropped/No. of packets forwarded
Step : 11- Calculate Path Trust
PT = $\sum NT$
Step : 12- Sort(PT)
Step : 13- Send data according sorted path
Step : 14- Stop

A new routing algorithm is used for prevention of black hole attack in the network by trust based multipath routing algorithm.

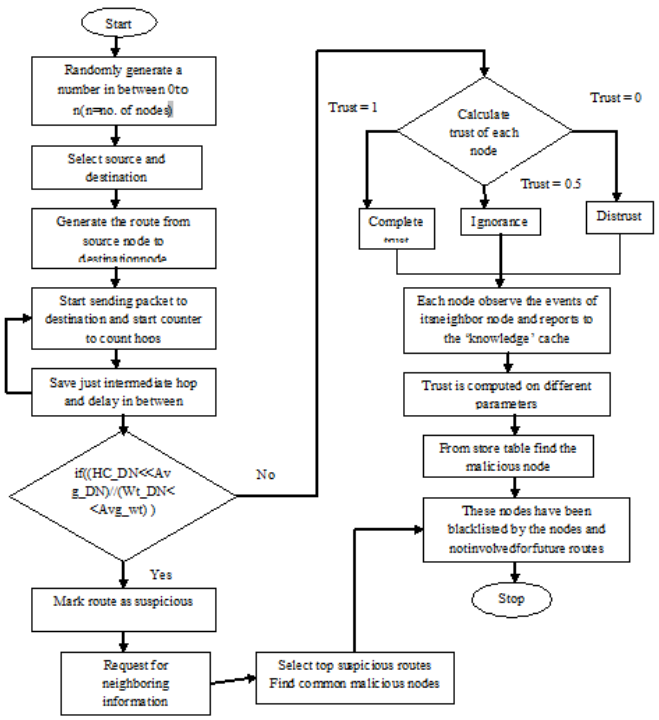

Fig. 3: Flowchart of proposed work

VI. RESULT ANALYSIS

In this we have compared the results of proposed trust based multipath routing algorithm with existing method. To check the performance of our protocol we have comparedit with the AODV protocol under effect of BH attack. The node and there speed is variable and also the number of BH nodes. By changing the number of nodes and BH nodes we studied the performance of our protocol. In table 1 represents the simulation parameters with its values.

TABLE 1: SIMULATION PARAMETERS

Parameters	Value
Channel_type	Wireless_channel
Radio_propagation_model	Two_ray_ground_model
MAC_type	802.11
Antenna_model	Omni directional antenna
Number_of_mobile_nodes	30
Routing_protocol	AODV, BHAODV, IDSAODV
Simulation area	300*300
Simulation duration	100 sec.
Maximum speed	40-120 m/s
Transport layer protocol	CBR(UDP)
Data payload	512 bytes
Packet rate	10kb/s

Dropped packet:

In fig 3, depicts the comparison between existing method and proposed trust based multipath routing protocol with respect of packet drop rate. It represents that packet drop are high in the proposed method.

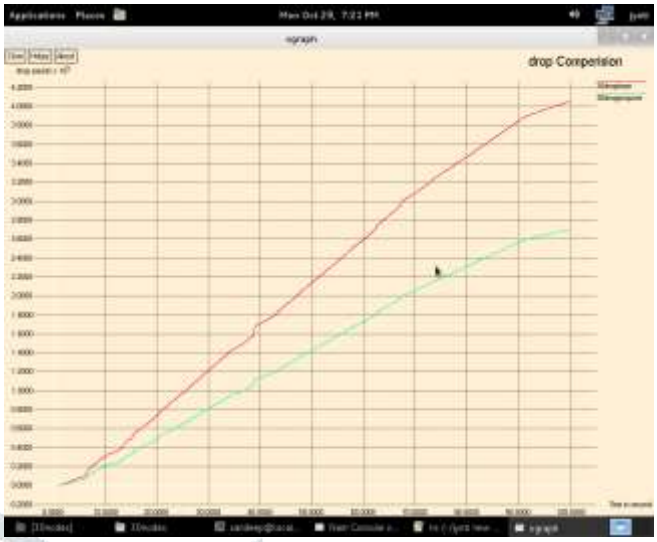

Fig. 3: packet drop comparison

Packet sent:

How much packetsare forwarded to the destination shown in fig. 4. In this forwarded packet are greater in compare of previous method.

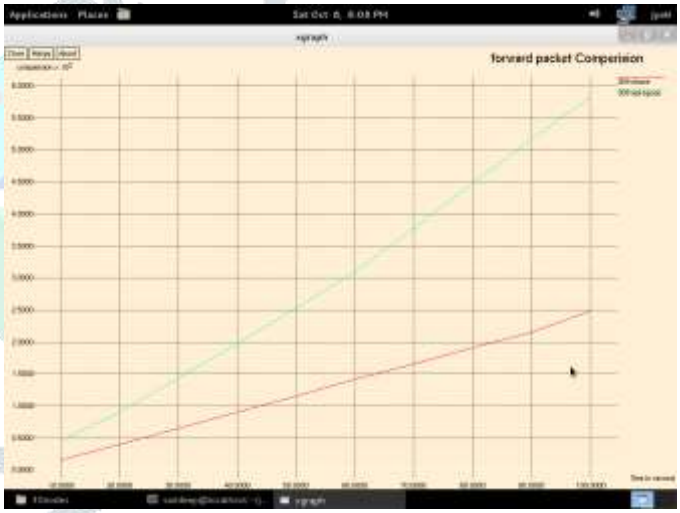

Fig. 4: forwarded packets

Routing overhead:

It is the whole wide variety of control packets inside the network at some stage in the transmission of data from source to destination. The graph shows that the routing overhead is high in the proposed work which is less in existing technique in fig. 5.

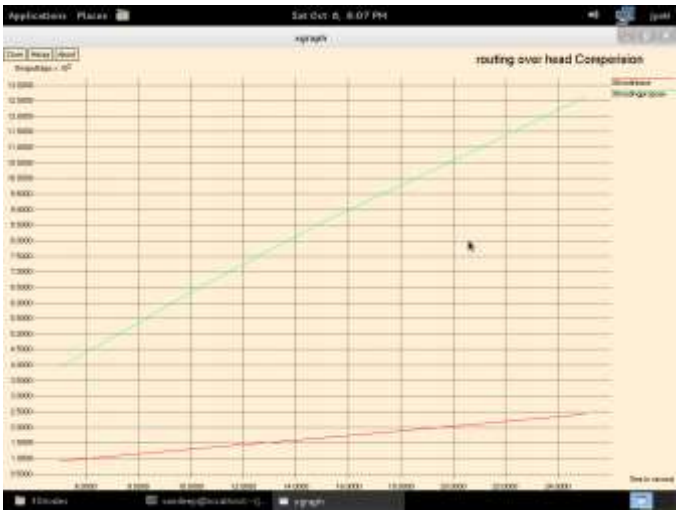

Fig. 5: routing overhead

Packet delivery ratio:

It is the definition in which the total numbers of received packets calculated in terms of sent packets. It is in the percentage form which has no unit. The graph shows that a PDR graph among base method as well as proposed method. This PDR rate is greatest in projected than previous method.

PDR = Total received packets / Total sent packets

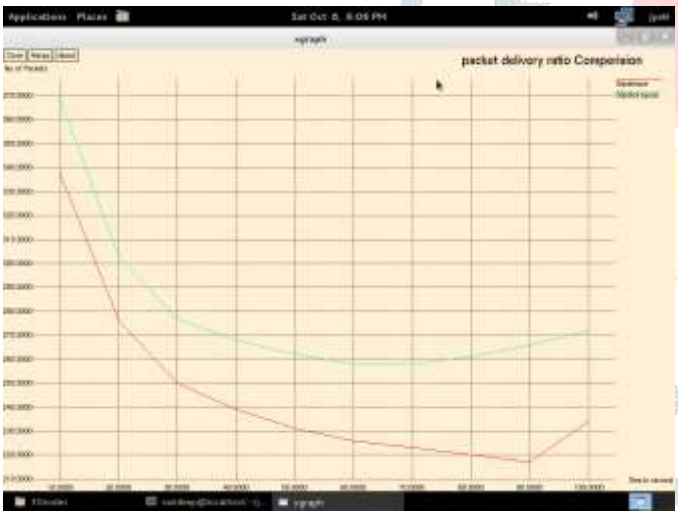

Fig. 6: packet delivery ratio

In fig. 6 display the packet delivery ratio in the network. Here, graph define packet delivery ratio are greater in compare of existing method.

VII. Conclusion

AODV is vulnerable to the well-known black hole attack. Black hole attack is one where any of the service can be denied. When there exists a black hole node in network, then reliable data transfer cannot be guaranteed. Hence nodes with greater need for communication, suffers a lot.In ad hoc network we have limited resources whichcomplicate the detection process. Trust based multipath routing is used as our proposed method. Simulation results have defined the throughput and packet delivery ratio is improved and malicious node can be easily identified in the network.

REFERENCES

[1] Tripathi, A., & Mohapatra, A. K., "Mitigation of Blackhole attack in MANET", 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), 2016, pp. 437-441.

[2] Mohite, V. G., & Ragha, L., "Security agents for detecting and avoiding cooperative blackhole attacks in MANET", 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2015, pp. 306-311.

[3] A.Kannammal and S.Sujith Roy, "Survey on Secure Routing in Mobile Adhoc Networks", International Conference on Advances in Human Machine Interaction (HMI - 2016), IEEE, 2016,pp. 1-7.

[4] Bala, A., Bansal, M., & Singh, J., "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications. 2009, pp. 141-145.

[5] Wakode, N. G. (2017). Defending blackhole attack by using acknowledge based approach in MANETs. 2017 International Conference on IoT and Application (ICIOT).

[6] Kamel, M. B. M., Alameri, I., & Onaizah, A. N. (2017). STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET. 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC).

[7] Dumne, P. R., & Manjaramkar, A. (2016). Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs. 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).

[8] Abdelshafy, M. A., & King, P. J. B. (2016). Resisting blackhole attacks on MANETs. 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC).

[9] Arya, N., Singh, U., & Singh, S. (2015). Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. 2015 International Conference on Computer, Communication and Control (IC4).

[10] Patidar, K., & Dubey, V. (2014). Modification in routing mechanism of AODV for defending blackhole and wormhole attacks. 2014 Conference on IT in Business, Industry and Government (CSIBIG).

[11] Dangore, M. Y., & Sambare, S. S. (2013). Detecting and Overcoming Blackhole Attack in AODV Protocol. 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies.

[12] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad Hoc Networks. 2012 Second International Conference on Advanced Computing & Communication Technologies.

[13] G. Stephanie Vianna et al, "Trust Based Approach to Overcome Black Hole Attack in Manet", International Journal of Pure and Applied Mathematics, Volume 118, No. 22, 2018, pp. 1763-1769.

[14] Siddharth Dhama et al, "Black Hole Attack Detection and PreventionMechanism for Mobile Ad-Hoc Networks", International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2016, pp. 2993-2996.