International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 05 (SEPTEMBER -OCTOBER, 2017)

Trusted path selection for resistance of black-hole Attack in MANET

MD Shamsul Haque[1], Prof. Deepak Singh Tomar[2]
M. Tech. Scholar, Department of CSE,
TIT, RGPV, Bhopal, India.
[1]Sam4u1985@gmail.com, [2]tomar_deepak01@yhoo.in

Abstract— **Mobile Ad hoc Network is generally a self-organized networks and intermediate nodes must perform end-to-end communication in between sender to receiver in dynamic environment. To achieve this, each node depends on its neighbor to forward the data packet to the destination. The MANET is easily organized at any place where the mobile devices are available for communication. In fact, most of previous studies on MANET have implicitly assumed that nodes are cooperative and without cooperation it is not possible to establish connection for sending data in dynamic network. The Black hole attacker in MANET are easily affected the routing performance by that the data receiving proportion is affected as compare to normal network performance and dropping of data is improved. In this research we proposed new IDS (Intrusion Detection System) of detecting routing misbehavior of Black hole attack. The property of black hole attack is to reply the positive acknowledgement to destination at time of route request and drop all the data packets at the time of data sending. The proposed secure is identified the attacker behavior in two stages. In first stage the IDS nodes are only finding the suspicious node and the final decision of attacker confirmation is decided by the Head node. The Head node is instructing the IDS to finding attacker from suspicious having data receiving is less than 70%. Then the IDS nodes are wedge the communication of attacker and give the safe communication among the mobile nodes with improvement in data receiving.**

Keywords:-MANET, Routing, Black hole, IDS, Head Node, Packet dropping.

I. INTRODUCTION

The design goal of Mobile ad hoc networks technology is to support web access anyplace and anytime, with none pre-defined infrastructure that supports the quality of the users, wherever network intelligence is placed within each mobile device. Attributable to its self-configuration and self maintenance capabilities MANETs will have many varieties of applications like rescue operations, military and security operation, conferencing, enforcement and residential network. Mobile ad hoc networks are infrastructure less during which nodes are liberal to move Associate in attention to deploy them in a discretional fashion [1]. Two nodes will have multiple links between them for communication and deployed in an exceedingly complete fashion, appropriate for price and time effective setting, and for a scenario wherever infrastructure is troublesome to setup. Security is difficult in MANETs attributable to its characteristics like peer to see design, operational while not central arranger, dynamic topology, insecure operational setting, and frequent link breakage attributable to mobile nodes, battery period of time, machine capability and non uniformity. Communication in MANETs is thru single hop in link layer protocols and multi hop in network layer protocols, supported the belief that each one the nodes in an exceedingly network are cooperative in coordination method, however sadly this statement isn't true in hostile setting. Malicious attacks will simply disrupt network operation by violating protocol specifications .The network layer operation in MANETs are supported routing and knowledge packet forwarding each are susceptible to malicious attacks. Routing in MANETs is classed as Reactive (On demand) Routing and Proactive (Table driven) Routing. A reactive protocol initiates routes whenever they're required whereas proactive protocols maintain consistent and up-to-date tables that contain routing info from every node to each different node. During this paper we have a tendency to be considering reactive routing protocol like AODV. Since no security mechanism is provided by AODV, attack will be performed by any malicious node by disobeying the protocol specifications. The key AODV vulnerabilities are Deceptive incrementing of Sequence Numbers and decrementing of Hop Count. region attack is Associate in Attention attack during which all the packets in an exceedingly network are redirected to a particular node that incorrectly claims to possess contemporary route, and absorbs or drops those packets while not forwarding them to different or destination nodes.

II. LITERATURE SURVEY

[1]Mohamed A. Abdelshafy, Peter J. B. King, "Resisting Black hole Attacks on MANETs" The title we discuss a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal protocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior. We present a Black hole Resisting Mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol. It does not require expensive cryptography or authentication mechanisms, but relies on locally applied timers and thresholds to classify nodes as malicious. No modifications to the packet formats are needed, so the overhead is a small amount of calculation at nodes, and no extra communication. Using NS2 simulation, we compare the performance of networks using
AODV under black hole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a black hole attack.

[2] Sathish M, Ad hoc On Demand Distance Vector (AODV) routing is an extensively accepted routing

protocol for Mobile Ad hoc Network (MANET). The inadequacy of security considerations in the design of AODV makes it vulnerable to black hole attack. In a black hole attack, malicious nodes attract data packets and drop them instead of forwarding. Among the existing black hole detection schemes, just a few strategies manage both single and collaborative attacks and that too with much routing, storage and computational overhead. This paper describes a novel strategy to reduce single and collaborative black hole attacks, with reduced routing, storage and computational overhead. The method incorporates fake route request, destination sequence number and next hop information to alleviate the limitations of existing schemes.

[3] Siddharth Dhama, in the mobile Ad-hoc networks, there exists various challenges in packet data delivery mechanism. Therefore transferring data from one node to other node is challenging. One of such attack is the black hole (BH) attack in a network. We are proposing a mechanism for the detection and prevention of BH attack in the mobile ad hoc network. The routing protocol that 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 false information to the sender. In this paper we not only preventing but also detecting the BH node. The simulator used here to implement the mechanism is NS 2 and result proved the effectiveness of model as the throughput is very high as compared to AODV that does not have proposed mechanism.

[4] Dhiraj Nitnaware, Dynamic MANET On-Demand (DYMO) routing protocol has been used to establish an ad-hoc networks. DYMO is advance version of AODV routing protocol develop to improve the network performance. Security is the major challenge in DYMO routing protocol and prone for various security threats. This research work attempts to develop a mitigation algorithm to avoid and prevent genuine nodes from malicious attack. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. The black hole node presents itself in such a way to the other nodes and networks that it knows the shortest path. The complete research work is classified into three categories which are without attack, with attack and preventive scenario. The performance parameter taken for analysis are throughput and packet delivery ratio against the varying parameters like number of nodes, speed, pause time and area to observe the impact of black hole attack and proposed mechanism with different situation. A Qualnet 5.2 simulator has been used to simulate and evaluate the performance of proposed solution. The complete experimental setup concludes that improvement in mobile node increase the network performance but also increase the black hole impact. Subsequently, improvement in node speed degrades the black hole impact.

[5]Bhavana K S, Ravi P "Resistance of Black hole Attacks on Manet's With The Support Of Modified Dynamic Source Routing Protocol" Due to the enhancement in the field of technology there is a vast improvement in the field of communication, which led to the changes in the medium from, wired to wireless medium. One of them in mobile ad-hoc network. The wireless medium which has many advantages like low resource consumption, high performance, capability and so on. Since it is a wireless there is a security breach in the network. The security threats may include black hole attack, grayhole attacks & other attacks. These attacks cause denial of services which decreases the performance. This paper includes the mechanism called as black hole resisting mechanism, which includes neighbor identification fake request transmission, original request transmission, route discovery and optimal route selection. By adopting these schemes we can detect the black hole nodes & exclude them prevent the attack.

[6] Nigahat, Dr. Dinesh Kumar, "Black Hole Detection And Prevention Using Aodv And Shortest Distance Technique" we discuss a Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Proposed work includes the detection mechanism for black hole attack and mechanism to prevent the black hole attack in MANET using Advanced Ad-Hoc on Demand Distance Vector (A-AODV) protocol.

III PROPOSED WORK

Mobile ad-hoc network is a growing field due to easy deployment of network anywhere and anytime. Mobile ad-hoc research open to design new routing strategies, security and processing capability of devices that's why numerous researches done on the field of define methodology. In this dissertation resolve the black hole attack through two level of security approach in first level neighbor node identifies the activity of established path after that send the report to the next level of security approach, where collaborative manner taking the decision about black hole node blocking based on attack behaviors. In the previous research different strategies apply to resolve the problem of black hole attack with different routing strategies i.e. AODV, DSR and DSDV etc. In the base paper they proposed black hole resistance module under AODV routing and analyze and compare with AODV-S mechanism they found BRM their proposed approach gives better outcomes. From the previous approach found that some refinement are needed, that's why design a new trust based path selection method for resistance of black hole attack under mobile ad-hoc network. The proposed approach split into two phases detection and prevention from black hole attack, during the black hole detection process single detector node are watch the activity of its neighbor

and check the activity of connected nodes i.e. routing table, number of data receives, forward, drop, drop reason etc. While the detector node found that neighbor node generate the higher sequence number and flood the route request packet and also drop the incoming data by loop condition, than set as black hole suspicious node and sends the report to next level of security module for take decision of blocking the attacker node and new route establishment module. In the second level of security namely prevention module that take the input from different detector nodes and calculate the trust level of suspicious node by collaborative manner (multiple nodes calculate multiple trust value i.e. number of generated route packets, number of data drop by loop condition, overhead of particular nodes, processing capability utilization etc.) and calculated trust value, if average trust value less than 70% and data drop by loop condition that means particular node confirm that black hole and block the particular node. After the blocking of attacker node by collaborative decision making system, blocking message broadcasted in the network so that no one communicate through the attacker node. Proposed collaborative decision making system also call the local route repair module from ad-hoc on demand distance vector routing and joint the disconnected link by shortest path based mechanism, that work helps to minimize the delay of new path establishment process and decreases the overhead with lightweight mechanism.

1.1 Proposed Algorithm

In this section describe the proposed algorithm that optimized the existing security approach and improve the network performance in all aspect of network parameters. Algorithm provides the flow of execution in step by step process that describe by formal and informal way. By the informal way describe through sentence based approach that is follows.

The deployment, node initial position, movement, radio zone, routing strategies all the initial parameter describe in tool command language (tcl) script of all mobile node after that they invoke the AODV routing strategies define in NS-2 and establish the shortest path from source to destination, during the routing decision phase any one execute the black hole attack module than those node generate the higher sequence number and gain the channel and data. But our security module detects by detection module and report to the collaborative decision making system, these collaborative decision making system provide the decision about black hole node behavior and trust information and based on its trust value block the attacker nodes and established new path from source to destination. This above description describe in formal way is as follow.

Algorithm: Trusted path selection for resistance of black hole Attack in MANET

Input:

M: mobile node
S: source nodes
R: receiver nodes
I: Intermediate nodes
Ψ= radio range 550m
AODV: routing protocol
B: black hole node (0 to 10)
S_i: Suspicious nodes
D: detector nodes (1 to 6)
C: set of decision making nodes
t: trust value (initial 0)
r_pkt: route packet
R_table: routing table
h_seq: high sequence number

Output: NRL, packet delivery ratio, routing overhead, throughput, delay, attacker node.

I. Procedure:

Step1: S execute AODV routing
AODV generate routing packet
AODV(S, R, r_pkt)
Step2: **if** I in Ψ & I != R **than**
I← as a intermediate node
R_table(S, I)
if R_limit exceed **than**
Route not found
Else
Goto step 2;
End if
Else if I in Ψ & I == R **than**
R found
R_table (S, set of I, R)
Send acknowledgement to S
Call send (data, S, R)
End if
Send (Data, S, R)
Step3: Check route from S to R
Step4: if route exist than
Send data via I node
D watch the neighbor I node
Step5: **if** I drop the data by Loop || (I generate the h_seq && Broadcast (m-1) nodes) **than**
D set I node as a S_i
Send report to C(S_i, time, activity)
Else
Calculate t of I node
t = (data forward/ data receives)*100;
setp6: **if** t > 70 and drop != loop **than**
I work as normal
R receives data by selected path
Else
goto step 5;
End if
End if
End if
Step7: C (S_i, time, activity)
Receive the report from D
Step8: **if** S_i receives data by i-1 & S_i forward < 50% of receives than
Ci calculate (new t_r of S_i = old t_r – (number of forward/ number of receives))
End if
Step9: if drop == loop **than**
Cj calculate (new t_d of S_i = old t_d – (loop/total drop))
End if
Step10: **if** route sequence number == high **than**

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 05 (SEPTEMBER -OCTOBER, 2017)

Ck calculate (new t_s of S_i = old t_s – (number of h_seq generated by S_i/total number of h_seq generated by all node))
End if
Step11: calculate average trust of s_i
t of S_i = ($t_r + t_d + t_s$ / number of participated C)
if t of S_i < 70 % **than**
S_i set as B node
Block the S_i node
Broadcast $S_{i\ blocking}$ message to M-1 node
End if
C execute local route repair
Find new shortest path from S to R
Stop

IV Simulation Environment & Results Analysis

This section represents the overview of simulator tool and discuss about the results that evaluated after applying the proposed scheme.

A. Overview of Network Simulator

NS2 is a free simulation tool, which can be obtained from [7]. It runs on various platforms including UNIX (or Linux), Windows, and Mac systems. Being developed in the Unix environment, with no surprise, NS2 has the smoothest ride there, and so does its installation. Unless otherwise specified, the discussion in this book is based on a Cygwin (UNIX emulator) activated Windows system.

NS2 source codes are distributed in two forms: the all-in-one suite and the component-wise. With the all-in-one package, users get all the required components along with some optional components. This is basically a recommended choice for the beginners. This package provides an "install" script which configures the NS2 environment and creates NS2 executable file using the "make" utility.

1) Simulation Parameters:-

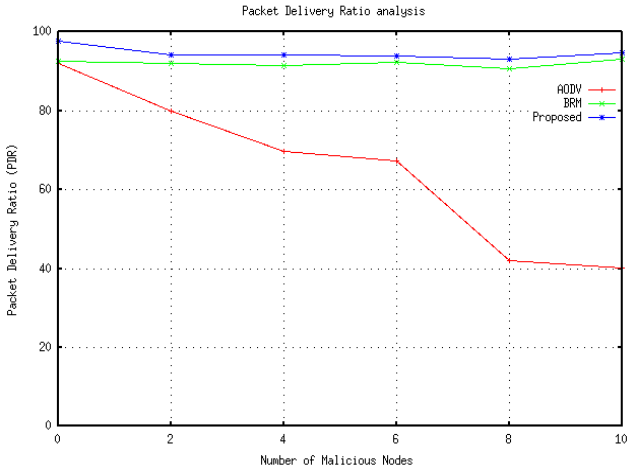
We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc. According to below table 1.1 we simulate our network.

A. Packet Delivery Ratio Analysis

Packet delivery ratio is the ratio of the packet that is successfully delivered to the destination compared to the no. Of packet that are sent by the sender. The Packet Delivery Ratio analysis is the total study of the packet delivery ratio of all the scenarios. The analysis shows the number of malicious node in X axis compared with probability of the packets delivered to the destination. The result analysis shows three different conditions normal condition, BRM and Node Trust based which is our proposed. The red line in the graph shows the probability of the packet delivery ratio with AODV routing protocol having black hole attack. The green line in the graph shows the probability of the packet delivery ratio when network uses BRM black hole prevention mechanism. Comparing the existing BRM black hole prevention mechanism with proposed Node Trust based module there is slight variation in the results but the proposed Node Trust based module has the higher packet delivery ratio as compared to the existing BRM black hole prevention module.

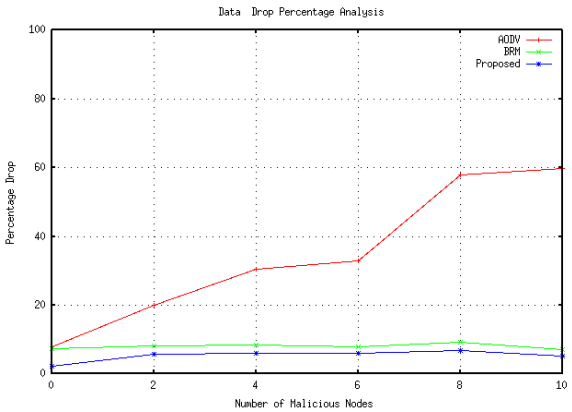
TABLE 1.1 Simulation Parameters for Case Study

Dimension of simulated	1200m×1200m
Routing Protocol	AODV
No of Malicious Node	0-10
Simulation time (seconds)	100
Attack Type	Black hole
Prevention Mechanism	BRM, Node Trust based
Transport Layer	TCP ,UDP
Traffic type	CBR , FTP
Packet size (bytes)	512
Antenna Type	Omni Antenna
Node Speed (m/s)	0 - 25 m/s



B. Percentage of Data Drop Analysis

Percentage of Data Drop Analysis is the ratio of the packet that is not delivered to the destination compared to the no. Of packet that are sent by the sender. The Percentage of Data Drop Analysis is the total study of the packet that is not delivered. The analysis shows the number of malicious node in X axis compared with probability of the packets delivered to the destination.

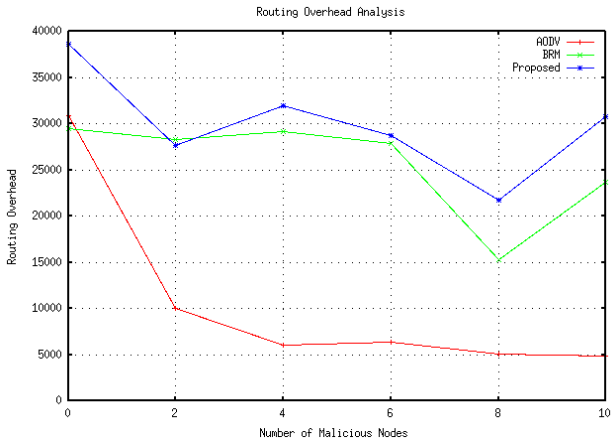


The result analysis shows three different conditions normal condition, BRM and Node Trust based which is

our proposed. The red line in the graph shows the percentage of the packet drop ratio with AODV routing protocol having black hole attack. The green line in the graph shows the probability of the packet drop ratio when network uses BRM black hole prevention mechanism. Comparing the existing BRM black hole prevention mechanism with proposed Node Trust based module there is slight variation in the results but the proposed Node Trust based module has the lesser packet drop ratio as compared to the existing BRM black hole prevention module.

C. Routing Overhead Analysis

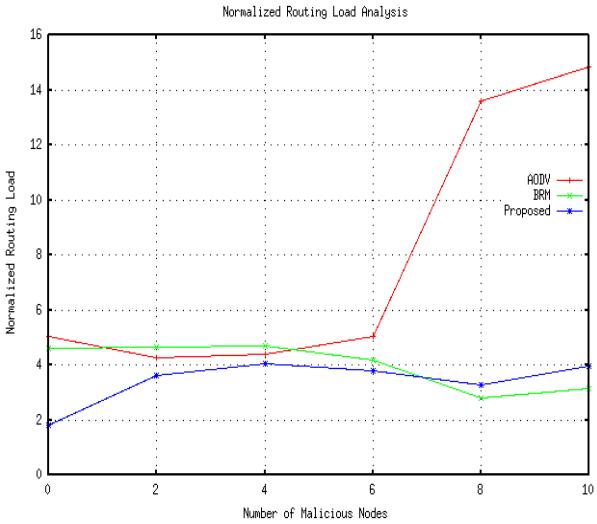
The number of packets flooding in network is required to establish connection in between sender to receiver. The sender is identified destination through connection establishment packets and these packets are confirm to sender, is destination is ready for receiving data in dynamic network. The energy is also consume in flooding of routing packets and also the network other resources are consumed that's why the minimum amount of routing packets flooding is better for better routing performance. The number of routing packets flooding in proposed routing is very less. The analysis shows the number of malicious node in X axis compared with routing overload in the Y axis. The result analysis shows three different conditions normal condition, BRM and Node Trust based which is our proposed. The red line in the graph shows the routing over load for the AODV protocol under black hole attack. The green line in the graph shows the routing over load for the BRM black hole prevention mechanism. The blue line shows the routing over load for the proposed Node Trust based module.



The routing packets flooding of the proposed Node Trust based module is really shows more flooding of data but black hole is shows reduction in flooding but data packets receiving is also very less in network. The BRM black hole prevention mechanism secure network and improves network performance after blocking attacker malicious function. The energy consumption is also reduces to prolong network life time. Comparing the existing BRM black hole prevention mechanism with proposed Node Trust based module there is slight variation in the results but the BRM black hole prevention module has the lesser routing packets flooding ratio as compared to the proposed Node Trust based module. This is due to large no packets are being delivered in the proposed Node Trust based module then the BRM black hole prevention mechanism.

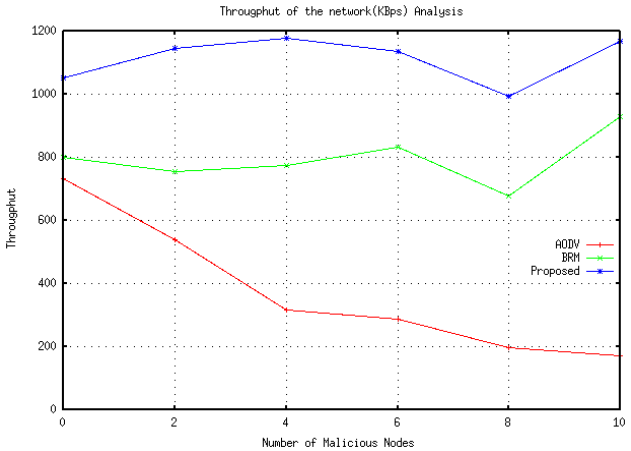
D. Normal Routing Load Analysis

Normal routing load is ratio between number of routing packets with number of data receives by the receiver, while the normal routing load (NRL) is greater that means network overhead is large, in this graph nrl value of AODV routing is higher because in this time no defensive mechanism exist but the proposed algorithm gives low overhead as compare to AODV.



E. Throughput Analysis

The number of packets is received at destination in per unit of time are measured the through throughput parameter. The throughput is higher in network, if the transmission and receiving are running continually without any hindrance like jamming and congestion. The analysis shows the number of malicious node in X axis compared with throughput in the Y axis. The result analysis shows three different conditions normal condition, BRM and Node Trust based which is our proposed. The red line in the graph shows the percentage of the packet received per unit time with AODV routing protocol having black hole attack.

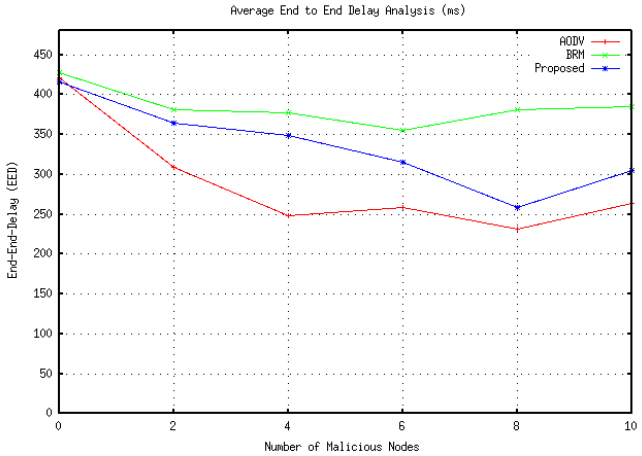


The green line in the graph shows the percentage of the packet received per unit time when network uses BRM black hole prevention mechanism. The normal condition is represented by the red line shows that the throughput for the network is low. The proposed methodology is

represented by the blue line in the graph. The throughput for the proposed methodology is greater than the other two conditions. This shows the proposed methodology work with less hindrance in the network. The overall analyses represents that the performance of the proposed methodology is better than the old and jamming condition.

F. Average End to End Delay Analysis

The end to end delay is the average time taken by the data packet to reach to the destination. The delay caused by route discovery process and the queue in the data packet transmission is also counted. The data packets that are successfully delivered to destination are only counted.



The analysis shows the number of malicious node in X axis compared with throughput in the Y axis. The average end to end analysis shows three different conditions normal condition, BRM and Node Trust based which is our proposed. The red line in the graph shows the average end to end with AODV routing protocol having black hole attack. The green line in the graph shows average end to end delay, when network uses BRM black hole prevention mechanism. The normal condition is represented by the red line shows that the throughput for the network is low. The proposed methodology is represented by the blue line in the graph. As in the graph the existing network is represented by the red line showing the average end to end delay. The proposed condition is represented by the blue line in the graph. The proposed methodology has less ends to tend delay as compared to the existing condition.

VI Conclusion

The security is the major issue in any network and in network it is necessary to provides security because most of the hosts are not authorized and also performing malicious activities in network. The mobile nodes in MANETs can moves freely in the lack of a fixed infrastructure unit. As a result, frequent changes in routes may happen due to unpredictable topology changes and link disconnections. Another one is nodes in MANETs has limited resources such as energy, bandwidth, and computational power of nodes and MANET has no trusted centralized authority. The proposed IDS method is not only detect the black hole attacker but also prevent the network from it. In this research the double verification system of attacker identification is more reliable and confirms the attacker presence after confirmation of all checker nodes. The IDS nodes are finding the first suspicious nodes and these suspicious nodes are declare as the attacker after conformation of data delivery less than 70%. The trust based approach is first filter the suspicious nodes then the nodes are confirm after the verification and decision of all IDS nodes under the control of **Head Node** in dynamic network. The whole security responsibility is of Head Node and all IDS nodes are monitor by **Head node**. The proposed IDS is improves the routing performance and provides the secure communication. The information of attacker is broadcast to all the nodes that are participating in routing procedure and these nodes are ignores the request of attacker if it identified again after block their existence. The performance of network in term of data receiving is improves and dropping of packets are reduced. The loss due to presence of attacker is completely removed and throughput and PDR of network improves. The double security system is enhance the reliability of trust factor and also reduces the time consumption to find attacker after continuously watching the activities of mobile nodes or key exchange encryption and decryption methods.

The characteristic of MANET is a decentralized network and forming dynamic link. The control in nodes movement and security is only possible through some better routing scheme and reliable routing scheme. In future we try to propose the security scheme against wormhole attack and flooding attack. The attacker identification is not only based on packet loss but also based on heavy packets flooding in MANET.

References

[1] Mohamed A. Abdelshafy, Peter J. B. King, “Resisting Black hole Attacks on MANETs” 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC).

[2] Sathish M, Arumugam K, S. Neelavathy Pari, "Detection of Single and Collaborative Black Hole Attack in MANET", IEEE WiSPNET 2016 conference.

[3] Siddharth Dhama, Sandeep Sharma, Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", 2016.

[4] Dhiraj Nitnaware, Anita Thakur, "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET", 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN).

[5] Bhavana K S, Ravi P “Resistance of Black hole Attacks on Manet’s With The Support of Modified Dynamic Source Routing Protocol” International Journal For Technological Research In Engineering Volume 4, Issue 9, May-2017.

[6] Nigahat, Dr. Dinesh Kumar, “Black Hole Detection And Prevention Using Aodv And Shortest Distance Technique” ijesrt Nigahat *et al.,* 6(4): April, 2017.

[7] The Network Simulator – ns-2. [Online]. Avalable: http://www.isi.edu/nsnam/ns/.