International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20 (2017) pp. 9245-9252

Adverse effect of Black hole and Worm hole attacks on MANETs

Dr A. Ramesh Babu
Professor & Head Department of Science and Humanities
Hindustan Institute of Technology & Science, Rajiv Gandhi Salai, Old Mahabalipuram Road,
Padur, Kelambakam, Chennai, Tamil Nadu 603103, India.
Orcid Id: 0000-0001-5795-3871

M V S S Nagendranath
Research Scholar, Department of Computer Science and Engineering ,
Hindustan Institute of Technology & Science, Rajiv Gandhi Salai, Old Mahabalipuram Road,
Padur, Kelambakam, Chennai, Tamil Nadu 603103, India.
Orcid Id: 0000-0001-9550-1067

Abstract

The underlying component that supports the device communication within the Manet is that the wireless connection capability. Each node has the flexibility to communicate with alternative nodes via the creation of routing path. However, due to the actual fact that nodes in Manet are autonomous and also the routing methods created are only based on current condition of the network, some of the ways are very instable. In light of those shortcomings, several analysis works emphasizes on the development of routing path algorithm. inspite of the appliance the Manet will support, the Manet possesses distinctive characteristics, that allows mobile nodes to make dynamic communication regardless the availability of a fixed network. but the inherent nature of Manet has led to nodes in Manet to be susceptible to denied services. A typical packet drops in Manet is that the black hole attack and worm hole attack caused by a misbehaviour node, or a group of nodes advertising false routing updates.

Typically, the malicious nodes are tough to be detected. every node is equipped with a specific kind of routing protocol and voluntarily participates in relaying the packets. However, some nodes might not be genuine and has been tampered to behave maliciously, that causes the black hole attack, worm hole attack. many routing protocols are vulnerable to such attack.

In this theory, the attack exploits the Route Request (RREQ) discovery operation and falsifies the sequence number and also the shortest path info. The malicious nodes are ready to utilize the black hole within the RREQ discovery method owing to the absence of validation method. As a result, genuine RREQ packets square measure exploited and mistakenly relayed to a false node(s). This paper highlights the effect black hole nodes, worm hole nodes to the network performance and therefore substantiates the previous work done [1]. during this paper, many simulation experiments are iterated using NS-3, that used varied eventualities and traffic loads. The simulation results show the presence of black hole nodes, worm hole nodes during a network will considerably affects the packet delivery ratio and throughput by the maximum amount as 100%.

Keywords: MANET, AODV, Worm Hole, Black Hole, Simulation, NS-3.

INTRODUCTION

The Mobile ad hoc Network (MANET) technology is extraordinarily dependable on the reliability of communication among devices. every node in manet is provided with a wireless ad hoc routing protocol, capable of sending information to different nodes. The data, which may be within the type of text or voice are sent to destination i.e. server to be analyzed. However, the communication usually depends on extremely reliable wireless ad hoc connectivity. Some nodes are mobile, which can be integrated with vehicles to gather traffic parameters. Such communication ability is presently offered by Manet. however, a number of the security options in Manet are weak and may be exploited. a major highlight of the ad hoc network as compared to the normal wired networks is that the ability produce communication path on dynamically. in addition, the nodes will freely move within the network, whereas being connected.

The network offers a self-organized topology, autonomous and decentralized multi-hop wireless system of mobile nodes [2][3]. Such attributes change users to easily deploy the network for emergency necessities. it's additionally appropriate for short term desires and may be created to hide special areas wherever forming a wired network infrastructure isn't viable. Therefore, the network finds application in fields like disaster relief operations, transport networks, military science communications, environmental observation. Figure one shows a straightforward operation of Manet, wherever the destination is outside the radio vary of the source node. a group of mobile devices between the pair of source and

destination nodes, inter-operates to relay packets. every intermediate node often checks the shortest path to destination once receiving the RREQ. In MANETs, every node might act as a router or a bunch for information transmission and depends on the establishment of multi-hop routes to overcome the restrictions of their communication range.

The network is versatile and nodes equipped with similar routing protocol will be part of and leave the network. because of mobility, a routing path often breaks and it poses a good challenge to maintain consistent network property. To support the property between nodes in MANETs, routing protocols like AODV [4], (DSDV) [5] are used to establish paths within which packets are propagated throughout the network. However, because of the high separation distance between a combine of source and destination nodes, different nodes assist to relay the packet, as shown in Figure one. In several analysis works, [5][7][8] the communication model presumes that the intermediate nodes will assist to hold data traffic from different nodes, and thus, nodes exchange data and control packets based on mutual trust. nevertheless, during a highly open system like Manet, the lack of validation mechanism for identifying real packet causes the system to be vulnerable to security threat.

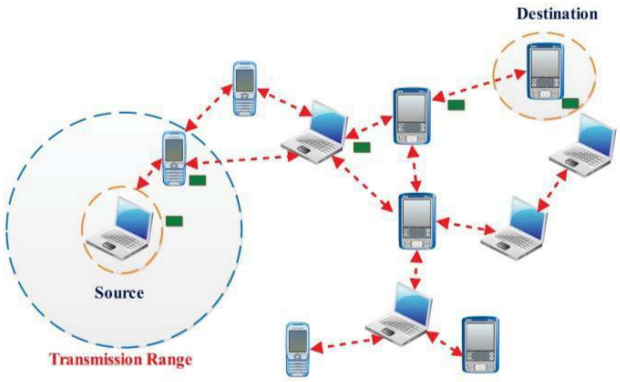

Figure 1: Multi-hop Mobile Ad hoc Network

Generally, security ambushes in Manet are requested into two classes, that are active attacks and passive attacks. In active attacks are done to start data from sort out like, spying attacks and development stream examination ambushes. Undoubtedly, unapproachable aggressors get information changed inside the framework however not irritating the operation of a framework and alteration information. However, in powerful strikes, replication, alteration and cancellation of changed information is done by aggressors. each active and passive attacks will be also subdivided into two classes i.e. attacks outside to the framework and inward to network. Inside attacks are done by certified center point inside the framework, however external ambushes are executed by center points that they're not embraced to share inside the framework decisions. Another request of attacks is ensured to tradition stacks, for example, orchestrate layer ambushes. Figure 2 shows the gathering of security threats on Manet.

The wormhole attack, sinkhole attack, Gray hole, black hole attack, to name a few, are some of the most important instances of DoS attacks that may be dispensed in MANETs [12]. The common attribute of the previously declared DoS attack is that the malicious node falsifies the update info within the propagated packet. however, during this paper, the main target is to detect black hole and wormhole attack in AODV protocol.

The AODV is chosen as the base routing protocol for the analysis as a result of the protocol share several characteristics with different on-demand-routing protocols. In addition, the essential feature of AODV doesn't include any validation mechanism to see for real packet. because of such deficiency within the AODV algorithm, the malicious operation of the black hole nodes is implemented and therefore the impact to the network performance will be investigated.

Some AODV options also are similar with different on demand routing protocol and changes to the AODV will be adopted by other MANETs routing protocols with minimal changes

Figure 2: Classification of security attack

In the black hole attack, the malicious node generates and propagates false routing information and advertises itself as possessing a legitimate shortest path to the destination node. As shown, once the malicious node advertises the routing information to the requesting node before the real node, a false route are going to be created. As a result, packets might not be ready to reach to the particular destination node [12][13]. The false routing updates broadcast by the malicious node ends up in packet drop and so, causes sub-optimal network performance. Moreover, once multiple malicious nodes get together to create an attack the degradation to network performance are going to be more vital. this is often called a collaborative black hole attack.

Basically, the vulnerability of AODV routing protocol are due

to the absence of the validation mechanism to visualize for malicious node. based on this vulnerability, the black hole node is ready to leverage on such weaknesses and exploit the mutual trust communication between nodes. after, the receiving nodes will be deceived by the malicious node and therefore the harm to the network will be simply executed.

Numerous studies have tried to enhance security strategies for on demand routing protocol [14][15][7]. However, many of the projected schemes have only marginally improved the network performance. it's as a result of the schemes fail to accommodate the dynamic attributes of MANETs i.e., topology, different network sizes, variable battery capability, error prone medium, power, storage and process resources[4]. Such challenges have created it difficult for previous researchers to design a fixed and efficient routing protocol.

In this paper, five different types of DoS attack generally found in Manet are expressed.

- Wormhole Attack: throughout this attack, an attacker node records a packet, at one location at intervals the network, tunnels the packet to a unique location and replays it there.
- Sinkhole: during a sinkhole attack, a compromised node tries to draw in information from the neighboring nodes. it is done by promiscuously eavesdrops every information that's being communicated between its neighboring nodes. Upon receiving the information, the packets are dropped causing high network loss and packet retransmission by the supply node.
- Gray-hole Attack: throughout this attack, the router that's mesh behave simply not well and a group of packets are forward and handle by receiver but leave by others. The presences of these attackers are exhausting to watch in wireless networks as a result of over the wireless link the packets are lost due to bad channel quality[10].
- Replay Attack: it's a malicious attempt by the attacker, that collects information and routing packets. Later the collected packets are replayed. Such attack might cause a network to be incorrectly detected and it permits unauthorized users to impersonate a distinct node identity. usually such technique is employed to realize access to information that was demanded by replayed packet.
- Black hole Attack: The offender advertises a zero metric for all destinations, leading to all nodes inside the proximity to route packets towards it. A malicious node sends fake routing data, claiming it's an optimum route and causes completely different nodes to route information packets through the malicious one. later, every packet routed through the malicious node is dropped[7].

The aim of this paper is to analyze the performance of Manet exploitation AODV routing protocol with and whereas not the presence of black hole attack, worm hole attack. The AODV routing protocol is chosen as a results of the actual fact it fulfil the on demand routing behavior. it's jointly equipped with each unicast and multicast routing capabilities. The paper is organized as follows. Section 2 provides an outline concerning AODV routing protocol and collectively discusses the region,worm hole attacks. Section 3 discusses the security mitigation. Section four presents the simulation methodology. Section four discusses results and conjointly the performance analysis. Section five concludes the paper.

AODV ROUTE REQUEST AND BLACK HOLE

AODV Route Request

AODV is classed as a reactive routing protocol. it's one of the most well-known protocols in manet, that inherits variety of the options of Destination Sequenced Distance Vector (DSDV) routing protocol[13]. In contrary to DSDV, the AODV route request procedure is changed to reduce the quantity of broadcasts. The routes are established on-demand compared to DSDV, wherever complete lists of routes are maintained upon the primary route request

Almost like DSDV, the AODV routing protocol employs the destination sequence vary to keep up each route entry. before broadcast, the destination sequence vary is generated by the destination node[21]. to keep up contemporary path, the requesting node selects the route supported packet that carries the simplest sequence range. Basically, the AODV has three message varieties, that are RREQs, Route Replies (RREPs), and Route Errors (RERRs). Upon receiving the RREQ, a node 1st checks in its routing table for existing path back to the sender. If such path does not exist, the node then generates an entry for a reverse route. On the opposite hand, if the node's table shows a legitimate reverse route entry but the sequence range could be a smaller amount than the source sequence range among the RREQ (a larger vary suggests that fresher information), this reverse route entry is changed with the information among the RREQ[8]. If a node contains a path to the destination, and conjointly the route is not terminated, the node will instantly reply with unicast RREP packet back to the supply by mistreatment the reverse path. however, the RREQ will still be propagated until it reaches the destination[8]. Note that the destination node will follow a similar mechanism as antecedently declared once it receives the RREQ packet[35].

Black Hole Attack

Black hole attack will severely deteriorate the manet and it's performed by one node or a mix of nodes [17]. In associate

ad-hoc network that uses the AODV protocol, a black hole node pretends to possess up to date routes i.e., greatest sequence selection to all or any destinations requested by the sender eventually absorbs the network traffic. once a supply node broadcasts the RREQ packet, the part node directly responds with associate RREP message that choices the simplest potential sequence vary, that is perceived originates from a real destination or from a node that comes with a recent enough route to the destination. The supply assumes that the destination is behind the half node and discards varied incoming RREP packets. once the supply node receives the RREP packet, it then starts to send the knowledge packets to the part node trusting that these packets can reach the destination. Eventually, the knowledge packet is born and not propagated further to the important destination.

As shown in Figure 3, the source node A broadcasts AN RREQ message to go looking out a route to the destination node F. AN RREQ broadcast from node one is received by neighboring nodes a mix of, E and D. However, as presently as a results of the request packet is received by the malicious node M, it sends AN RREP packet despite the absence of valid path to the destination node F. Forward the RREP message from the malicious node M is that the initial to arrive; the supply node updates its routing table for the new route to the particular destination node and discards any RREP message from varied neighboring nodes beside the one from the particular destination node[6]. Once the supply node stores a route, it starts causing data packets to a malicious node expecting that the knowledge can reach the supposed destination node. yet, the malicious node (performing a district attack) drops all data packets instead of relay to ulterior hop[8] [14].

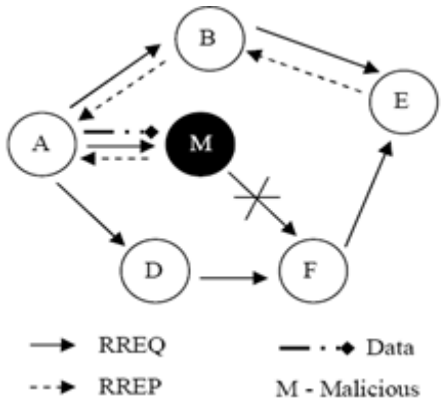

Figure 3: AODV Black Hole attack

Worm Hole Attack

Wormhole strike generally relates a join of remote poisonous center points showed up as X and Y in Figure-4. X and Y every unit related by methods for a wormhole associate which they hope to strike the source center point S. all through way finding theory, S conveys RREQ to an objective center D. Subsequently, An and C, neighbors of S, make due with RREQ and transmit RREQ to their neighbors. before long the convulsive center point X that gets RREQ sent by A. It records and entries the RREQ by methods for the quick exhaust associate with its assistant Y. Noxious center Y propels RREQ to its neighbor B. Finally, B propels it to objective D.

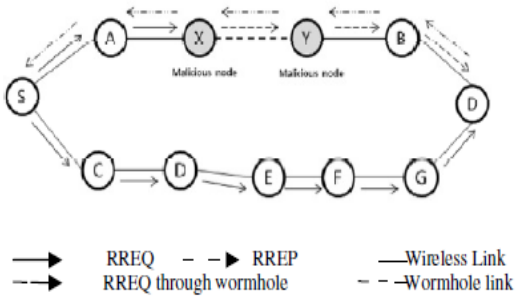

Figure 4: AODV Worm Hole attack

Thusly, RREQ is sent by methods for S-A-X-Y-B-D. On the backwards hand, totally startling RREQ allocate what's more sent through the trail S-C-D-E-F-G-D. Regardless, as X and Y unit related by methods for a quick transport, RREQ from S-A-X-Y-B-D accomplishes first to D. In this way, objective D ignores the RREQ that accomplishes later and picks D-B-A-S to unicast a RREP package to the source center S. Hence, S picks S-A-B-D course to send information that, so experiences X and Y malicious center points that are greatly all around put stood out from various centers inside the framework.

Thusly, a wormhole ambush isn't that proficient to mastermind, however still are generally unendingly perilous for a Manet. Furthermore, finding higher methods for acknowledgment of wormhole ambushes and securing AODV against in any case them remains an outsized test in Mobile Ad-hoc Networks

SIMULATION EXPERIMENT

The simulation experiment is conducted based on parameters shown in Table 1. Basic operation of Black Hole node is illustrated by Figure 4 and such attack are simulated on multiple scenarios with different topologies. In general, a Black Hole attack is assumed when data packets are dropped due to false updates. In this experiment, a known number of malicious nodes are introduced and data is collected at the specific malicious nodes. Therefore, dropped packets due to route breakages and interference will not be accounted. In that way, accurate results can be shown to differentiate the performance of MANET under severe malicious node attack.

Figure 5 shows when a source has data to transmit to an unknown destination.

Table1: Simulation Parameters

Network Parameters	**Values**
Number of Nodes	20,40,60,80,100
Number of Black Hole Nodes	0 to 3
Simulation Time	600 sec
Simulation Area	1000m x 1500m
Routing Protocol	AODV
Simulator	NS-3 (version 3.25)
Traffic	CBR
Pause Time	2 s
Speed	30
Packet Size	512 bytes
Mobility Model	Random Waypoint
Number of Scenario	750
No of Connections	1 to 20
Physical Layer	IEEE 802.11b
MAC Layer	802.11

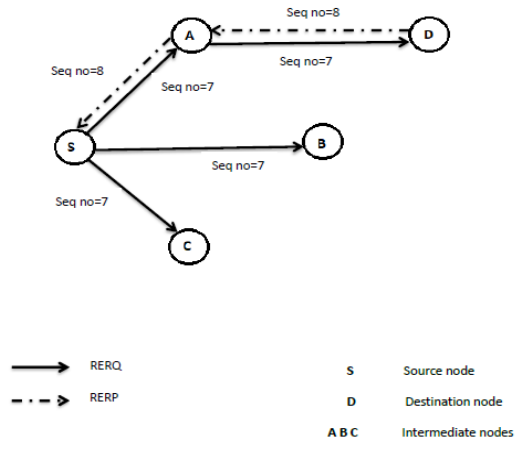

Figure 5: AODV packet transmission process

Results and Performance Analysis

The simulations parameters utilized in NS3.25 for the performance analysis with and while not the black hole attack are tabulated in Table1. a complete of 125 completely different eventualities with numerous node positions, quality and speed has been simulated and tested with the presence of 0 and 3 black holes. to make sure the results are credible, the confidence level issue is enclosed within the analysis. every information is computed and results are given with error bars. the confidence interval was computed based on Equation 1 and Equation 2.

$$s = \sqrt{\frac{n\sum_{t=1}^{n} x_t^2 - (\sum_{t=1}^{n} x_t)^2}{n(n-1)}} \qquad \text{Equation-1}$$

$$\bar{x} \pm t\alpha/2 \frac{s}{\sqrt{n^t}} \qquad \text{Equation-2}$$

Where x = Average

t = Coefficient Interval

s = Standard deviation

n = Sum of experiment

Margin of error = t*s

The metrics accustomed assess the performance are shown below:

1) Packet Delivery ratio: Packet Delivery ratio (PDR) is that the ratio between range of packets transmitted by a traffic source and conjointly the amount of packets received by a traffic sink[2].
2) Average End-to-End Delay: The packet end-to-end delay is taken into consideration as a result of the common time a packet takes to traverse the network. this is often the time from the generation of a packet by the source[2].
3) Throughput: the common rate at that the data packet is delivered successfully from one node to a unique over a communication network, output is usually measured in bits per second (bits/sec)[14].

TP = (Number of delivered packet * Packet size)

Figure 6 shows the result of black hole nodes on the PDR. it's clear that the impact of malicious activities within the network will considerably degrade the packet transmission. during this specific experiment, every node is about to a set most speed of 10m/s. Despite the increase within the range of nodes, the PDR remains systematically higher for the network that is free from malicious activities. Similar performances also are discovered for the throughput and packet end-to-end delay, as shown by Figure 6 and Figure 7 respectively.

With 3 malicious nodes present within the network, the turnout is 100 percent lower as compared to the network while not malicious nodes. However, a little difference is discovered for the end-to-end delay, significantly once the amount of nodes is about to 40. This result could also be due to the characteristics of the movement pattern utilized in the

simulation. As will be seen in Figure 5 through Figure 7, the performance slightly dipped at 20 nodes. any investigations to the movement pattern files used shows that the source nodes are randomly set in proximity to the malicious nodes by the Bonnmotion. As a result, the performance for a network with 20 nodes systematically drops.

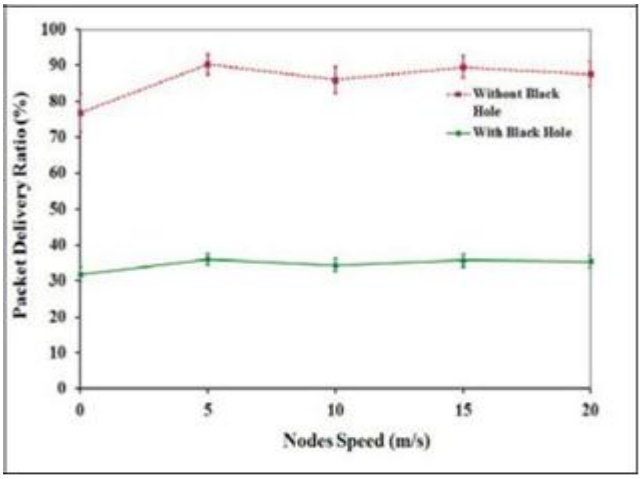

Figure 6: PDR with varying number of nodes

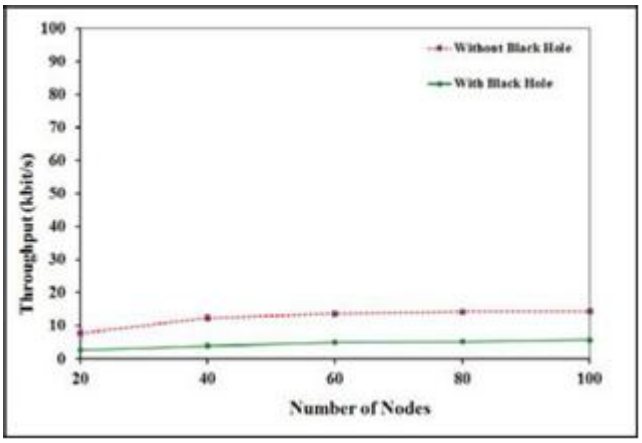

Figure 7: Throughput with varying number of nodes

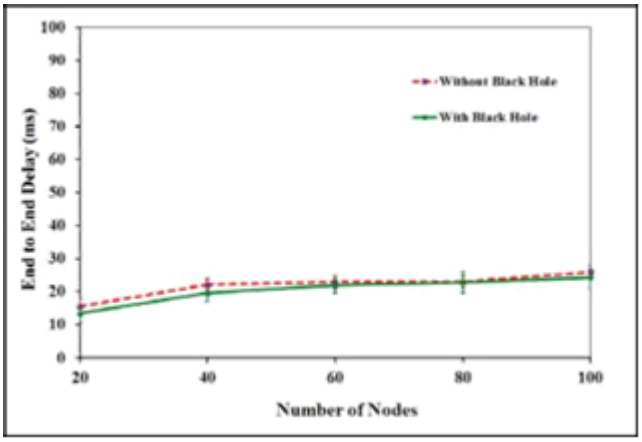

Figure 8: End-to-end Delay with varying number of nodes

Nevertheless, once the experiments are iterated with varied nodes speed, similar performances to the varied nodes are determined. The network with the presence of malicious nodes systematically shows sub-optimal performance as compared to the best network i.e. network free from black hole nodes. during this experiment, the entire numbers of nodes are set to 50, whereas the speed varies from 0m/s to 20m/s. As shown by Figure 9, the PDR for both networks significantly differs. The PDR of a network with malicious nodes drops twice the maximum amount compared to the network that's free from malicious nodes. The PDR is drastically reduced as a result of the amount of packets successfully delivered is considerably reduced. However, once nodes are mobile, the impact of malicious activities is additionally combined with the route breakage and path disconnection. Figure 10 shows the impact of the black hole attack to the networks throughput. it's measured that the throughput considerably decreases with the presence of the malicious nodes within the network. On the opposite hand, it's determined from Figure 11 that there's a small increase within the average end-to-end delay while not the result of black hole nodes, as compared to a perfect network. this is as a result of the inherent nature of malicious nodes, that immediate reply with the false fresh routes and after allows the malicious activities to be performed.

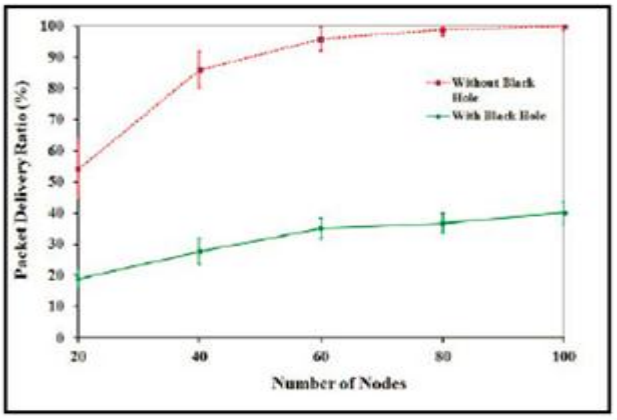

Figure 9: PDR with varying nodes speed

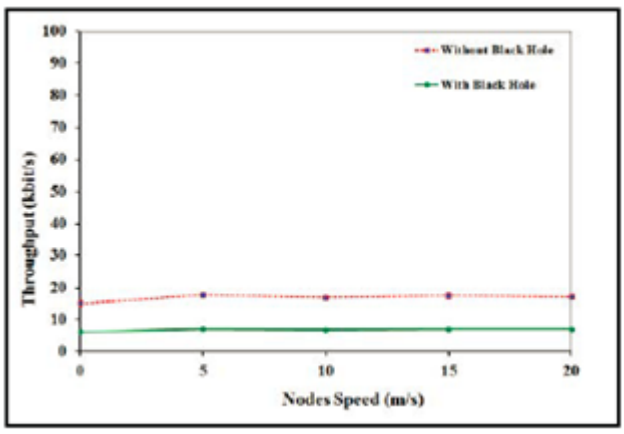

Figure 10: Throughput with varying nodes speed

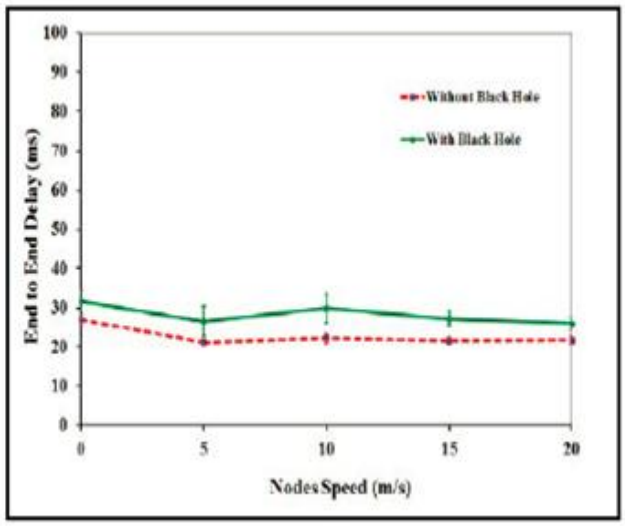

Figure 11: End-to-end Delay with varying nodes speed

CONCLUSION

In this paper, completely different mobile ad hoc network things are analyzed with and whereas not the presence of black hole attack supported the AODV routing protocol. The routing protocol performance is investigated with exploitation varied loads shown by the simulation parameters. subsequently the network is analyzed with altogether totally different performance metrics like packet delivery magnitude relation, average end-to-end delay, and outturn inside the deployed network. The simulation results signify that the performance of network inside the presence of black hole attack is preponderantly decreasing in packet delivery magnitude relation as a result of the attacker nodes discards all the info packets traversing its path. in addition the throughput well decreases once the network is given with malicious nodes. it's as a results of most of the packets sent do not appear to be delivered to the destination. the standard end-to-end delay slightly can increase whereas not the impact of black hole attack. this is often expected as a results of the malicious nodes instantly send reply whereas not conducting a check on its routing table. These changes inside the utilised metrics conclude that network performance degrades predominantly inside the presence of black hole attack. In future work, we have a tendency to tend to can simulate and analyse the impact of the black hole attack in a very larger network exploitation all completely different mobility models and compare its performance with the other on-demand-routing protocols.

REFERENCES

[1] A.T. Kolade, M.F. Zuhairi, H. Dao, and S. Khan, "Bait Request Algorithm to Mitigate Black Hole Attacks in Mobile Ad Hoc Networks," in Journal of Computer Science and Network Security, vol. 16, No. 5, 2016.

[2] K. S. Patel and J. Shah, "Study the Effect of Packet Drop Attack in AODV Routing and MANET and Detection of Such Node in MANET," in Proceedings of International Conference on ICT for Sustainable Development, 2016.

[3] C. Singh, "A Review: Comparative Study of Routing Protocols for Adhoc Networks," International Journal of Advance Research in Computer and Communication Engineering–IJARCCE, vol. 4, 2015.

[4] A. Ahmed et al., "AODV Routing Protocol Working Process" Journal of Convergence Information Technology, vol. 10, 2015.

[5] P. Mitra and S. Mukherjee, "A review of trust based secure routing protocols in MANETs," International Conference and Workshop on Computing and Communication (IEMCON), 2015.

[6] G.He, "Destination-Sequenced Distance Vector (DSDV) protocol," Networking Laboratory, Helsinki University of Technology, 2002.

[7] Mehdi Medadian and Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol" European Journal of Scientific Research Vol. 69 No.1 2012.

[8] Govind Sharma, Manish Gupta, "Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE).

[9] V. M. Agrawal and H. Chauhan, "An Overview of security issues in Mobile Ad hoc Networks," International Journal of Computer Engineering and Sciences Vol. 1, 2015.

[10] P.Chahal, et al., "Comparative Analysis of Various Attacks on MANET," International Journal of Computer Applications, vol. 111, 2015.

[11] M.Bhatt, et al., "Prevention and Detection of Black Hole Attack in MANET: A Survey," Imperial Journal of Interdisciplinary Research, vol. 2, 2016.

[12] R.H.Jhaveri, et al., "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad Hoc Networks," 2ndInternational Conference on Advanced Computing & Communication Technologies, 2012.

[13] Lalit Himral et. al.,"Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST).

[14] Maryam Gharooni et. al., "A Confidential RFID Model to Prevent Unauthorized Access" 3rd International Conference on Information Science and Engineering (ICISE2011), 2011.

[15] Niranjan Kumar Ray and Ashok Kumar Turuk,"Performance Evaluation of different wireless ad hoc routing protocols", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012.

[16] K. Lakshmi et. al, "Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology.

[17] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" Wireless Networks, Vol.11, 2005.

[18] Yongguang Zhang, Wenke Lee, Yi-An Huang "Intrusion Detection Techniques for Mobile Wireless Networks" Mobile Networks and Application, 2003.

[19] H. A. Esmaili, M. R. Khalili Shoja and Hossein Gharaee, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator," World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, 2011.

[20] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks”, International Conference on Wireless Networks (ICWN), 2003.p.1-7.

[21] S. A. Razak, S. M. Furnell, P. J. Brooke, “Attacks against Mobile Ad-hoc Networks Routing Protocols”, In Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting (PGNET), England: Plymouth; 2004.