International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Novel Preventive Detection Technique for Black-Hole Malware Attack in Wireless Mobile Ad-Hoc Network (WMANET)

Arun Kumar, Abhishek Kumar, Prashant Johri, Shiv Prakash, Tarun Kumar

Abstract-A wireless mobile ad-hoc network (WMANET) is endless self-organizing, infrastructure-less collection of movable devices which are connected by using a wireless communication system. In other word's WMANET is an autonomous, decentralized, dynamic topology, provisional network system having wireless movable devices (nodes) moving randomly without an infrastructure of the network. Furthermore, the nodes communicate with every supplementary node, through forwarding data-packets toward other nodes in the WMANET. The node finds a path to the destination node by applying routing techniques. Due to the dynamic topology of movable nodes wireless mobile network is more vulnerable to security and unprotected to attacks by the malicious node. One of the attacks is Blackhole malware Attack, a malicious-node wrongly advertises shortest to the destination node among an intention of disrupting the network communication. Because the data packets did not arrive at the destination node due to this attack data is lost. In the literature, researchers have been proposed various preventive detection techniques. These techniques used to detect and prevent the black-hole malware attacks. Furthermore, in this paper Novel Detection and Prevention mechanism (INCMAODV) has been simulated the black-hole attack in WMANET scenario. The proposed technique tried to find quality of service (QoS) parameters for instance throughput (Th), packet delivery ratio (PDR) and delay of the network and compared with the state of the art.

Keyword- Wireless Mobile ad-hoc network (WMANET), Security Attacks, Black-hole, Malicious-node, Security, Authentication, QoS Parameters, Throughput, Delay and Packet Data Ratio

I. INTRODUCTION

An Ad-Hoc Network is very useful on disaster recovery, military operations, smart building and so on due to some characteristic such as decentralized, dynamic topology, self-configuration, lack of infrastructure, self-organization, maintenance, quick deployment. WMANET is groups of wireless mobile devices where each device works as host with a router itself [5]. WMANET is an asset of mobile devices which may communicate with every node without whichever centralized system.

In this, when the nodes are want to communicate but the node is out of its radio range, that time it provides the multi hope communication otherwise it can connect directly. In WMANET every node gratis to join, leave and move randomly, independently and as result, we get very dynamic topology and unpredictably. Mobility leads to fluctuation in the link capability; high-bit error rate of system network connection is performed [2]. Due to the nonexistence of central control nodes are vital to collaborate among themselves. This flexibility of mobile nodes results in dynamic topology. Hence it is difficult to develop various routing protocol in WMANET as compared to the conventional wired network. An Ad-hoc network is very vulnerable so attackers easily attack it. Attacks in WMANET are basically in two classes: Passive attack, the attacker's id only stolen the useful information and does not affect the routing protocol. It is very difficult to find out. Inactive, attackers modify, delete the exchanging data or adversaries of exchange data to attract the packets and it also disturbs the routing protocol. It is very easy to find out and dissolve [6]. A number of routing protocol exists in the WMANET, but all are mainly categorized into three classes which are Proactive protocol, Reactive protocol, and Hybrid routing protocol. Proactive WMANET Protocol (PMP's), all nodes know about the all nodes information in maintaining a table called routing table. It guarantees that information is available to all nodes. Reactive WMANET protocol is provides routing paths only when it needed. In this not need to maintain the routing table and not need to analyse the best path scenario. When a route is required the system broadcast a route request RREQ message. These are transmitted instantly to connected routers that pass this request to the destination node and the destination node uni-cast with route reply RREP packet. The first reply path is used as a routing path [3]. The hybrid routing protocol can be defined as a mixture of advantages available in proactive and reactive routing techniques.

II. BACKGROUND AND TERMINOLOGY

Mainly WMANET uses two different types of routing techniques named as proactive and reactiveprotocol.

Manuscript published on November 30, 2019.
* Correspondence Author
Dr. Arun Kumar*, Assistant Professor in Centre for Advanced Studies Lucknow, India.
Abhishek Kumar, Assistant professor atAdwita Mission Institute of Technology (AMIT), Shivdham (Bihar) India.
Dr. Prashant Johri, Professor in School of Computing Science & Engineering, Galgotias University, Greater Noida, India..
Dr. Shiv Prakash, M.Tech. and Ph.D. School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India.
Tarun Kumar, Assistant Professor in School of Computing Science & Engineering, Galgotias University, Greater Noida, India.

One of the reactive routing techniques is an Ad-hoc on demand distance vector (AODV). AODV has the biggest advantage that it will not at operational state until it is required. AODV mainly maintain two different mechanisms which are route discovery and route maintenance till use.

The Route discovery is the process when the sender wants to communicate with destination due to unavailability of Route in the Routing Table. In this procedure, a Route Request (RREQ) packet is broadcasted into the network. If a node receives a fresh Route Request then first it will check I am the destination if yes then the packet is sent which consist the reply with own destination IP, the destination current sequence number etc. otherwise it will check in the routing table.

III. ATTACKS IN WMANET

In the literature, Fan-Huns Tseng et al [7] addressed the security attacks in WMANET. According to authors [1,2] securing the WMANET uses various methods is making sure mutual confirmation of participations nodes, confidentially and integrity of exchange-data availability of the network resource and access control to the network communication medium.

Attacks are mainly included attempting the drop or destroy the data packets, disturb or break the network, unauthorized access to the data or forged packets into the data streams.

Several types of attacks are identifying [7] in recent years in this fields some of them are discussed below:

A. Black-hole attack:

Attackers use the routing protocol to advertise it as having the shortest path with the greatest sequence number and smallest hope count. When an attacker receives the route request from the node it replies I have the shortest path and when inter in the node all commands go to the attackers and perform the denial of service (DoS) attack.

B. Wormhole attack:

A malicious node receives packets at one location in the network and tunnels them to another location in the network, where the packet resent into the network. This tunnel between two colluding attackers is referred to Wormhole attack.

C. Gray-hole attack:

In the gray-hole attack packets are drop due to denial of service attack; dropped each UDP packets, where forwarding the TCP attacks, dropping 50% of UDP packet. It is a loss of the network.

D. Information discloser attacks:

These attacks are specifically targeted to acquire system-specific information about a website such as software, distribution name, version number, and patch level. This obtained information may contain the location in the storage media having the backup file or the temporary file.

E. Byzantine attack:

A set of compressed node work in collusion and carry out packets, on non-optimal path selectively dropped packets. It is very hard to detect.

F. Resource consumption attack:

An attacker target to consume or wasted the resource of others nodes available in the network. Such as battery, computational power, bandwidth etc.

G. Packet modifying:

Contains the packet data is changed by the intermediate nodes. (H) Flooding attacks:

It is a denial of service (DOS) attack, in which a malicious node broadcasts the infected packets to the important network resources. Flooding attack is doable in all most each on-demand routing techniques.

IV. RELATED WORK

The routing problem is the fundamental problem. It is widely solved by many researchers in the previous decade. The first related work used in this paper is based on Support Vector Machine (SVM) Mechanism [1, 13-15] to identify malicious node in the black hole attack based on the performance of the intermediate nodes. Method called on using AODV technique, SVM method. This method observes behaviour of the node on the basis of the PDED (Pocket delivery ratio), PMOR (pocket modifying ratio) and PMSIR (pocket misroute ratio). The standard ratio (PDED<0.5, PMISR<0.2 and

PDER>0.7) defines for this above ratio on the basis of previous. So if node not follows the standard, that node is malicious node or black-hole.

Further in the literature [2,14-15,19-20] utilizes promiscuous mode to identify the malicious node and if yes, then broadcast the message that the malicious node is present in the system. Further, the intermediate node sends a PPER packet to the source node, then providing sent RREP packet to take switch on its promiscuous mode and send a "hello" message to the destination node through the intermediate node which is RREP packet is received. If this is legitimate node then to forward a message from this node to destination node else it is malicious node and broadcast message in the network. Further route of a source is refreshed by using table and try to a new route for again sending RREQ packet. Meenakshi et al. [3,16-17] proposed a novel method for detection and prevention of the WMANET flooding attack.

Further, this work utilized a Packet Delivery Ratio (PDER), Control Overhead (CO) and Packet Misroute Ratio (PMIR) conduct of the node to characterize the flooding attack. In this event the node can send RREQ packet without considering the RREQ_RATELIMIT within every second. Because of the flooding attack nodes course table full by the sham RREQ packet, so it not perform an activity on the genuine RREQ and misrouting the packet is considered to perused the behaviour and make a matrix to peruse it, by it author characterizes nodes are legitimate or malicious.

In [4,18-20] the authors built up a novel way to deal with keep away from the malicious node in WMANET. Because the malicious node shows that it has the best sequence number and most minimal hop count.

The proposed method, each RREP packet has additional three properties, for example, node ID, PPN number and group head ID. In this, every cluster head keeps up a neighbour table which keeps data about the entire node. Neighbour table keep up the node ID and cluster head ID.

Every node in the system has a particular prime number which goes about as node Identity and this character must not be changed. Thereafter, a novel technique depicted in the paper [5] called source routing discovery for preventing the black-hole attack (SRD-AODV) technique. Further, the researchers characterize the Threshold, least and most extreme number of nodes on the system. The Threshold id additionally characterizes in little, medium and expansive condition and has a malicious node in this condition separately 6%, 4%, and 2%. A malicious node dependably produces the best grouping number in light of the fact that malevolent don't have a clue about the goal arrangement number and if the succession number is more prominent than the aggregate number of node in the system so we effortlessly discover the malicious node or blackhole attack in the system. Here the author's contrast the malicious node succession number and the Threshold Number. In this process, if the sequence number is more noteworthy than the Threshold Number, it's a malicious node and needs to communicate that malicious node and re-broadcast the RREQ packet. In paper [6] the authors proposed a technique to identify the black-hole in the system by using an authentication method. This is a prevention method which uses an authenticated Hash function, message authentication code (MAC), and pseudo-random function (PRF) on the highest point of the AODV technique directing convention. It's a quicker way to deal with recognizable proof of a malicious node. The innovation that when RREP packet produced by the destination node at the time RREP packet encrypted and sends to the intermediate node with the public and private key. At each intermediate node take the packet and simply forward it. When it comes to at the source node at that point, it utilizes private key, opens the parcel. Prior to the open the bundle it checks the packet is same as the send packet. In the event that the message (RREP packet) is influenced then simply dispose of it and communicate the new RREQ packet to the neighbour node and communicate a message to distinguish a malicious node in the system. Various related security attacks are described in the works of literature are given as references [10-12].

V. PROPOSED METHOD

The Intermediates nodes Neighbours Comparison Method (INCM) technique read the behaviour of the neighbour nodes of the intermediate node on the basis of a sequence number and hops count, which is represented by figures 1 and 2. The network has many nodes; nodes are communicated with every other by sending the RREQ packet to its neighbours every neighbour reply with RREP packet when they got a route from the destination node. As the characteristic of the malicious node quick reply with the leading sequence number and least hope count. So source node understands this is the actual route to the destination and sends the data packets. In INMC, introduce a technique to prevent the black holes. In this first check, the neighbour's node of the 1st RREP intermediate node if the neighbour is destination node and then decides it's a malicious or not. If neighbour node is destination node then its again compare the sequence number and hop count of the 1st RREP node with the destination node and when it 1st reply nodes sequence number greater than the destination sequence number it also checks the hope count of the 1st reply with the destination node, both the condition is true then it's a malicious node and broadcast a message in network with the sequence ID of that node otherwise it's a legitimate node.

A. The Proposed Algorithm:

IF *(RREP nodes neighbour node is not a destination) then*
It's a malicious node and broadcasted in network with the sequence number as a black-holes.
Else
Compare RREP nodes sequence number and hop count with destination's the sequence number and hop count.

If *(RREP sequence number > destination sequence number) than*

If *(RREP hope count < destination hop count) than*

It's a malicious node and broadcasted the message in the network

Else
It's a legitimate node.

Else *It's a legitimate node.*

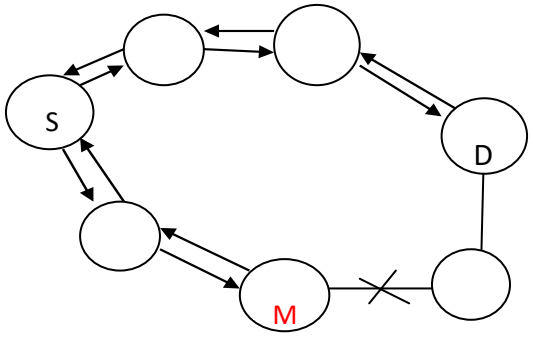

Fig 1-WMANET Attack Scenario 1

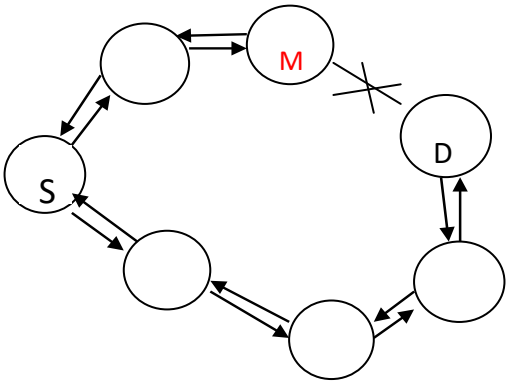

Fig 2-WMANET Attack Scenario2

VI. SIMULATION RESULT

A. SIMULATION MODEL

In comparison of theperformance of the AODV routing technique and AODV technique include with INCM technique in the term of Throughput, Delay and Pocket Drop Ratio (PDR) in case of Black Hole attack, the model of proposed solution and simulation parameters are describe in the table 1.

Modelling and Simulation of WMANET by using Network Simulator (NS-3)

In this section we had discussed modelling and simulation of the model using NS-3. In this paper IEEE 802.11 MAC layer [10] is used. The simulation experiment parameters are shown in table 1.

Table 1- The Simulation parameter using NS-3(V-2.35)

Simulation parameter	Value
Simulator	NS-3(V-2.35)
Techniques	AODV, INCMAODV
Simulation time	8 sec
Number of nodes	5,10,15,20
Transmission range	200m
No. of malicious nodes	2
Traffic type	UDP
Simulation area	1800* 840

The Performance Metrics: There are different types of parameters to evaluate the performance of WMANET routing techniques, which have different behaviours of the overall network performance. The overall performance will be evaluated on the three matrices: Throughput (Th), Packet Drop Ratio (PDR) and Delay (D). These matrices are defining follows.

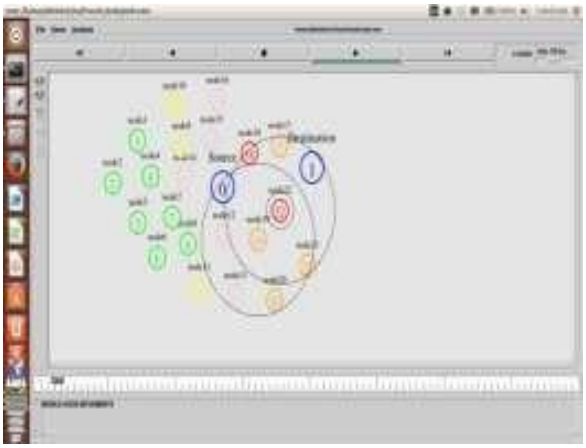

Fig 3- Test Simulation shows the two black holes in the network.

The Figure 3 depicts that the shortest route from source to destination. In figure 3 it is obvious that from source node 0 to destination node 1 there are two route first is node 18 node17 to node 1 and another is node 19 node 22 to destination node 1.

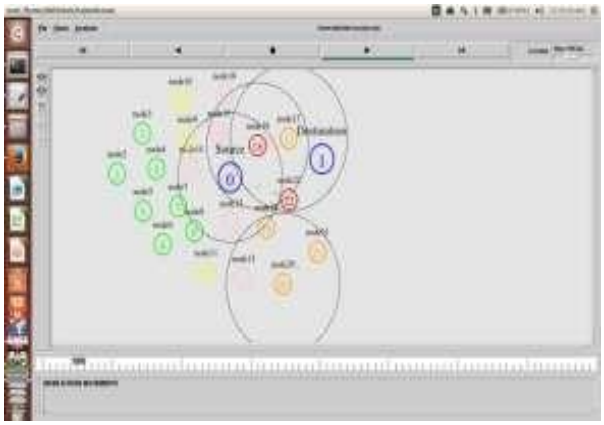

Fig 4-Data flow between node 0 to node 1 via node 18 and 17.

In figure 4 source (node 0) want to communicate with a destination (node1) so broadcast a RREQ message for finding the best route available in the network and wait for the reply. Here see that node 18 and node 22 as a black hole node or malicious node. When source node sends RREQ it first comes reply from the node 18 but node 18 (malicious node) so source do not know node 18 is legitimate node or malicious node because its sends reply with highest sequence number and minimum hope count so source node understand it is the shortest node to the destination and send the data packets and malicious node perform DoS attack on it. In this paper, three quality of service (QoS)

Thesecond quality of service (QoS) parameter is throughput (Th).It is defined as the number of bits transmitted to the higher layer in per unit time. Hence the data can be represented in form of bits per unit time can be calculated in terms of the rate of data successfully received bits from other stations in per unit time. The unit of Throughput is bits per sec.

Packet drop ratio (PDR) is another QoS parameter which is measured in form of the ratio of the number of data packets received at the destinations to the number of packets generated in the sources. Furthermore PDR can be given by mathematical, by following equation
parameters are addressed which are delay (D), throughput (Th) and packet drop ratio (PDR).

Thefirst quality of service (QoS) parameter is **Delay.** Delay can be defined as the end to end delay of each packets received by the WLAN MACs of each WLAN nodes in the communication network and transferred to the higher layer. This delay includes medium access delay at the source MAC, reception of each fragment individually.

$PDR = \frac{Pd}{Ps}$. Where, p_d is all data packets received at the each destination and p_s is all data packets generated the each source.

VII. SIMULATION EXPERIMENT RESULTS AND DISCUSSION

In this section the First it is compared the performances in terms of QoS Parameters viz. throughput delay (Th) and pocket delivery ratio(PDR) of AODV technique, and INCM technique versus number of nodes as shown in figures 5, 6 and 7.

In figures 5 it is clear that the pocket drop ratio increase(PDR) with increasing the number of nodes compare the AODV routing technique. In figure red line show the pocket drop ratio (PDR) of the INCMAODV technique and green show the pocket drop ratio of AODV routing protocol. New INCMAODV's technique PDR is less than the AODV routing technique.

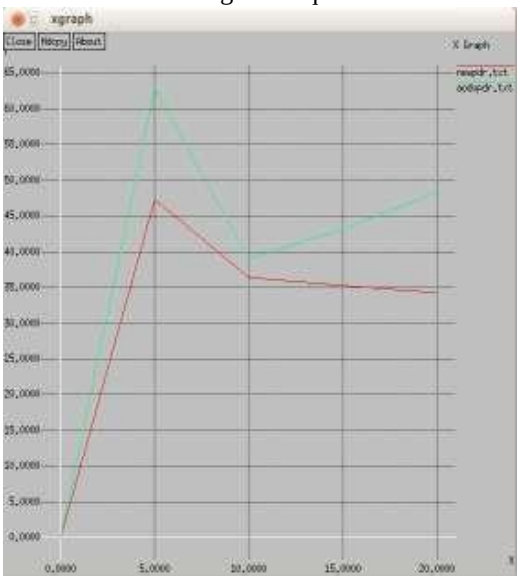

Fig 5-Comparison of Pocket drop ratio of INCMAODV with AODV routing technique

In below figure 6 see that the end-to-end delays (D) of the pocket received by the destination and generated by the source. For more efficient network it should be low as possible as. In figure at the time of number of node 5 and 10 it is greater than the AODV routing technique l but at no of node is 15 is decrease dramatically and smaller than the AODV technique. At the time no of node are 20 it goes approximately same to the AODV routing technique.

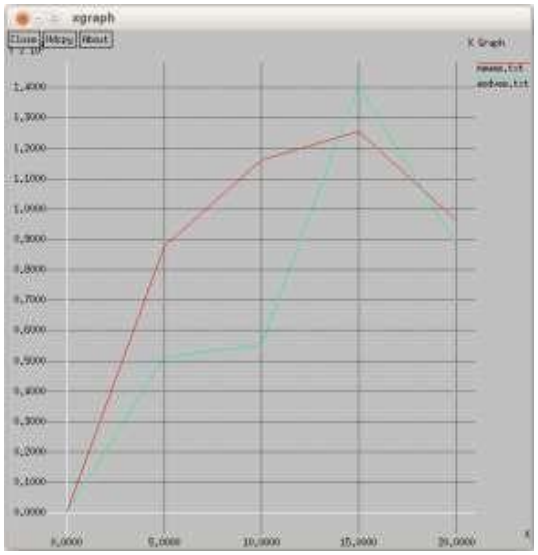

Fig 6-Comparison of the end to end delay of the INCMAODV and AODV.

Figure 4, Comparison of End-to-End delay(D) of INCMAODV technique and AODV routing technique. Throughput(Th) is a extremely important parameter for the any network. Throughput is depends up on the many parameters such as end to end delay(D), pocket drop ratio(PDR), pocket delivery ratio etc. if all of the parameters goes to high than throughput goes to high. Higher the throughput means more efficient network.

In figure below at 5 to 20 nodes INCMAODV's throughput is greater than the AODV. On the basis of throughput, INCMAODV technique is more efficient than AODV routing technique .

Fig 7 - Comparison of Throughput of INCMAODV with AODV

VIII. RESULT ANALYSIS

In this section all experiments designed in such way that each scenario consists of two simulation runs. In the first simulation run each node is running in a cooperative manner with other nodes to remain the network in communication with AODV technique. Further, in the various simulations having two malicious nodes carried out in which are the carrier of the
Blackhole Attacks.

In the present paper, we tried to perform the comparative study of the obtained results with node behaviours.

In this study, various qualities of service (QoS) parameters are evaluated. The first QoS parameter is the packet drop ratio (PDR). Hence we calculate the number of the packet are sent by the sending nodes and reached packet at the receiving nodes. In the proposed model section, we elaborate the calculation the for the obtained packets. Now we calculate the variation among the tables of standard AODV technique and Black-Hole AODV technique. Then the number of packets evaluated which not able to reach the destination node is fascinated in the Black hole Node. However, the packets lost (PD) in the Black-Hole Node are given in the 4th column of the table of the Black hole communication network. The enduring of the columns demonstrates the percentage of the packets lost (PD) and additionally in the table of Black Hole network, we supplemented a percentage of lost packets which are fascinated in the Blackhole Node.

Further, it is observed that the proportion of data loss of the blackhole AODV technique is increased further than the standard AODV technique simulations in each scenario. It is also obvious from tables 1, 2, 3 that the packet loss previously exists in the networks. The situation is as packets drop at the node interface queue due to the density of data traffic (PDR). Further, to optimize (minimize) the data traffic node is altered and packet parameters. Since the requirement to evaluate the Blackhole effect in the network, we have to reduce the packet loss which happens at the network, but the Black hole. In the WANET which does not have some Blackhole, the data traffic may be intense and packets may get lost, for example in FTP traffic. Further, the proposed model simulates of standard AODV technique, it is found that data loss is greater than before up to 40% when we alter parameters. Hence, the data loss does not forever declare there was a Blackhole Node in the network.

A. Performance Comparison Analysis with INCMAODV Technique

The result analysis of the proposed model has experimented with the NS-3 simulator for a WMANET having of 20nodes. It is presumed that there is one intruder transfer a sequence of successive packets with an attack to the destination node [14]. Further, the blackhole is considered detection state if the attack packets surpass through some of the nodes that comprise the blackhole enabled detection system.

For a defined experiment scenario use a certain set of 5 nodes from 20 nodes and experimented with an attack [10] and deem a sequence of five successive packets as with the attack technique signature. It is observed that the precision of preventive detection both in static and dynamic circumstance. It is not obvious in [10], how an attack that requires more than one-hop information gets detected but in INCMAODV technique\, multi-hop information is considered which overcome the limitation of the INCM technique. It has been observed a percentage of preventive detection of attack using INCM technique [10] of together a static and a dynamic node case, which was not present in the works of literature. Further the comparative study of the performance of INCMAODV technique and AODV technique further in terms of throughput. Therefore, consider that there are only two nodes in the simulation model. This node is randomly selected to be one of the nodes out of 20. Consider a system in which nodes that constitute the black hole detection system are chosen randomly. Figure 7: percentage of Detection shows the results for systems with no of Nodes 20 in Figure 7. The performance of INCMAODV is better than the AODV technique [10]. INCMAODV technique also detects single black hole detection for a static condition.

B. Throughput for AODV technique

Consider a network using AODV. Assume that the intruder is moving at a speed of 15m/s. We change the criterion used to determine the nodes that make up the black hole detection system. Use the same criterion as used in case of used in the static case. The only difference is that now the intruder is assumed to be mobile. Show the results for such a case in Table 2. Here INCMAODV technique also detects multimode black hole detection of a dynamic condition.

Table 2- The value of the all metrics in INCMAODV technique.

No of nodes	Pocket drop ratio (%)	Throughput (bps)	End to end delay (ms)
5	47.33	386.10	878.86
10	36.44	376.09	1163.40
15	35.24	369.14	1255.05
20	34.22	363.67	963.94

Table 3- Value of the all metrics in AODV routing technique.

No of nodes	Pocket drop ration (%)	Throughput (bps)	End to end delay (ms)
5	62.80	384.00	514.00
10	39.03	343.11	554.06
15	43.15	331.37	1410.84
20	48.35	347.30	882.91

The above table 3 presents the comparative study of throughput (Th) percentage among AODV technique and the proposed technique. Despite each value of a number of nodes, the throughput rate(Th) of the proposed technique is superior to AODV technique. Here the complexity of IDAODV technique is approximately equivalent to AODV technique.

IX. CONCLUSION

Analyse the effects of the black hole in an AODV technique and detection of it. For this purpose, we implemented an AODV technique that behaves as Black Hole in NS-3. We simulated four scenarios where each scenario has 5, 10, 15 and 20 nodes that use AODV technique also simulated the same scenarios after introducing two Black Hole Nodes into the network.

Moreover, implemented a solution that attempted to reduce the Black Hole effects in

NS-3 using and INCMAODV technique and simulated the solution using the same scenarios. Our simulation results are analysed below:

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. Simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole, Nodes increases then the data loss would also be expected to increase.

AODV technique in the network has normally 3.21 % data loss and if two Black Hole Nodes is introducing in this network data loss is increased to 92.59 %. If 3.21 % data losses already exist in this data traffic, Black Hole Node increases this data loss by 89.38 %. INCMAODV technique in the same network, the data loss decreased to 45.63 %.

These two results show that our solution reduces the Black Hole effects by 43.75 % as packet loss in a network using IINCMAODV technique and where there is no black holes increase to 75.62 %.

Using INCMAODV routing technique proposed mechanism increase the throughput 6.33% and this is more efficient than another method for detecting the black hole in WMANET. Another advantage is the decrease of pocket drop ratio is 26.14% comparison to AODV routing technique but end-toend delay increase 26.75% due to choosing another path as well as compare to the others parameters.

X. FUTURE WORKS

The future directions of this paper will be based on the black hole attack in the WMANET with INCMAODV routing technique simulation and then investigated its property. In the presented paper the AODV routing technique is applied. We can apply other techniques with its behaviour and comparative study of various techniques with a attack in WMANET. However, the dynamic routing techniques could be simulated too. The entire sets of routing techniques are likely to present dissimilar results. Consequently, the best routing technique to

Optimises (minimize) the Black-hole malware Attack possibly determined in the future.

REFERENCES

1. Nithya, B., Aishwarya Nair, and A. S. Sreelakshmi. "Detection of RREQ Flooding Attacks in MANETs." In Data and Communication Networks, pp. 109-121. Springer, Singapore, 2019.
2. Arulkumaran, G., and R. K. Gnanamurthy. "Fuzzy trust approach for detecting black hole attack in mobile adhoc network." Mobile Networks and Applications 24, no. 2 (2019): 386-393.
3. Pham, Thi Ngoc Diep, Chai Kiat Yeo, Naoto Yanai, and Toru Fujiwara. "Detecting flooding attack and accommodating burst traffic in delay-tolerant networks." IEEE Transactions on Vehicular Technology 67, no. 1 (2017): 795-808.
4. Dhende, Sandeep, Sandeep Musale, Suresh Shirbahadurkar, and Anand Najan. "SAODV: Black hole and gray hole attack detection protocol in MANETs." In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 23912394. IEEE, 2017.
5. Gurung, Shashi, and Siddhartha Chauhan. "A survey of blackhole attack mitigation techniques in MANET: merits, drawbacks, and suitability." Wireless Networks (2019): 1-31.
6. Desai, AneriMukeshbhai, and Rutvij H. Jhaveri. "Secure routing in mobile Ad hoc networks: A predictive approach." International Journal of Information Technology 11, no. 2 (2019): 345-356.
7. Khanna, Nitin, and Monika Sachdeva. "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs." Computer Science Review 32 (2019): 24-44.
8. Kumar, Vimal, and Rakesh Kumar. "A Cooperative Black Hole Node Detection and Mitigation Approach for MANETs." In International Conference for Information Technology and Communications, pp. 171-183. Springer, Cham, 2015.
9. Desai, AneriMukeshbhai, and Rutvij H. Jhaveri. "Secure routing in mobile Ad hoc networks: A predictive approach." International Journal of Information Technology 11, no. 2 (2019): 345-356.
10. Bakare, B. I., and J. D. Enoch. "A Review of Simulation Techniques for Some Wireless Communication System." International Journal of Electronics Communication and Computer Engineering 10, no. 2 (2019).
11. Kumar, Manish, Vanita Jain, Achin Jain, Uttam Singh Bisht, and Neha Gupta. "Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET." Journal of Discrete Mathematical Sciences and Cryptography 22, no. 2 (2019): 277-291.
12. Dilli, Ravilla, and P. Chandra Sekhar Reddy. "Robust Secure Routing Protocol for Mobile Ad Hoc Networks (MANETs)." In Innovations in Electronics and Communication Engineering, pp. 393-399. Springer, Singapore, 2019.
13. Luong, Ngoc T., Tu T. Vo, and Doan Hoang. "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks." Wireless Communications and Mobile Computing 2019 (2019).
14. Chen, Hongsong, Caixia Meng, Zhiguang Shan, ZhongchuanFu, and Bharat K. Bhargava. "A Novel LowRate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining HilbertHuang Transformation and Trust Evaluation." IEEE Access 7 (2019): 32853-32866.
15. Thivakaran, T. K., and T. Sakthivel. "GUARD: an intrusion detection framework for routing protocols in multi-hop wireless networks." Wireless Networks 25, no. 2 (2019): 819836.
16. Khanna, Nitin, and Monika Sachdeva. "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs." Computer Science Review 32 (2019): 24-44.
17. Jing, Xuyang, Zheng Yan, Xueqin Jiang, and Witold Pedrycz. "Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch." Information Fusion 51 (2019): 100-113.
18. Cui, Jin, Lin Shen Liew, GiedreSabaliauskaite, and Fengjun Zhou. "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles." Ad Hoc Networks 90 (2019): 101823.
19. Jing, Xuyang, Jingjing Zhao,Qinghua Zheng, Zheng Yan, and Witold Pedrycz. "A reversible sketch-based method for detecting and mitigating amplification attacks." Journal of Network and Computer Applications (2019).
20. Vigenesh, M., and R. Santhosh. "An efficient stream region sink position analysis model for routing attack detection in mobile ad hoc networks." Computers & Electrical Engineering 74 (2019): 273-280.

AUTHORS PROFILE

Dr. Arun Kumar, is working as Assistant Professor in Centre for Advanced Studies Lucknow, India. He received his M.Tech and PhD PhD in Computer Science from Jawaharlal Nehru University New Delhi, India. His research area includes Adhoc network, multimedia, cloud computing, information security etc. He is actively publishing in these areas. He is reviewer of several international conferences and international journals.

Abhishek Kumar, received M.Tech degree in Computer Science and Engineering (CSE) in 2014fromGalgotia University, India . His research interest includes, mobile ad-hoc networks, mobile computing, wireless network security issues. He is working as Assistant professor atAdwita Mission Institute of Technology (AMIT), Shivdham (Bihar) India .He has published 5 research manuscripts in different peer-reviewed national and international journals and conferences.

Dr. Prashant Johri, is working as Professor in School of Computing Science & Engineering, Galgotias University, Greater Noida, India..He has served as Chair in many conferences and affiliated as member of program committee of many conferences. He has supervised many PhD and M.Tech students. His area of research interests includes big data, data analytics, data retrieval and predictive analytics, information security, privacy protection, big data open platforms etc. He is actively publishing in these areas. He published several research papers in reputed international journal and conferences, he is also editor of many journal books.

Dr. Shiv Prakash, received M.Tech. and Ph.D. degree from the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India. His current research interest focuses on Internet of Connected Vehicles (IoV), Network Security. He is Reviewer of several referred International journals of repute (including ACM, IEEE, Taylor and Francis, Elsevier, Springer, Wiley, etc.).

Tarun Kumar, is working as Assistant Professor in School of Computing Science & Engineering, Galgotias University, Greater Noida, India. His current research area includes mobile computing, wireless sensor network, cyber security, machine learning and deep learning. He published several papers in reputed journals. He also organized and attended several workshops.