International Journal of Engineering & Technology, 7 (3.4) (2018) 84-89

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Defense Against Co-Operative Black-hole Attack and Gray-hole Attack in MANET

Niranjan Panda[1]*, Binod Kumar Pattanayak[2]

[1]*Department of Computer Science & Engineering, S'O' A*
[2]*Department of Computer Science & Engineering, S'O'A*
**Corresponding author E-mail niranjanpanda@soa.ac.in*

Abstract

Mobile Ad-hoc networks (MANETs) can be termed as an autonomous system created by the collaboration of a set of motile nodes communicating with one another through available wireless media and each node behaves as an end system, as well as a router for packet forwarding. Each node is allowed to move freely, change locations and configure them to form a network. Finding an optimal and efficient path between the sender and receiver node is the main aim of routing protocols. Multipath routing protocols show a better result in comparison to single path routing protocols, for data transmission from source to destination extending lifetime of the network. Along with that security in routing for a protected communication between nodes has become a prime concern as any attack during routing may interrupt data transmission, paralyzing the whole network. During packet transmission through multiple paths a number of attacks make come into action by the unauthenticated and compromised nodes present within the network and black-hole attack is one of them. So our objective is to design a multipath routing protocol that detects and avoids the path containing black-hole. Our paper proposes a way to defense the black-hole and gray-hole attacks with the help of intelligence in MANET.

Keywords: *Security; Attacks; vulnerabilities; Black-hole; Gray-hole; routing protocols.*

1. Introduction

MANET is gradually emerging to be one of the more novel and demanding area of wireless networking due to its increased demand in various applications areas that includes wireless sensor network (WSN), military application, disaster relief, collaborative and distributed computing, health and business. A set of autonomous wireless mobile nodes with self organizing capabilities assembled in an arbitrary and temporary network topologies, communicating over wireless links are referred as MANET. MANETs lack in resources from wired network and routing of information from source to destination node in such a resource constrained environment is a challenging task [1]. Initially the routing protocols try to discover an optimal path between communicating nodes present within the network keeping in mind about the constraints over the resources such as battery power, computational power and bandwidth of communication. Further routing protocols are designed based upon the metrics like hop count, transmission cost, residual energy of nodes etc. to provide better results [2]. For this purpose single path routing protocol like AODV [3], DSR [4], DSDV [5] etc. are used. During routing, selection of optimal path between the communicating nodes may reduce the energy of the nodes, further transmission of data through the same path may affects the network lifetime brutally making some nodes fail out of battery power [6]. Hence many researchers proposed a number of routing protocols that attempts to reduce the energy used by the nodes during routing for extending the lifetime of the network. [7-11]. Multipath routing schemes helps in selecting multiple number of paths between pair of nodes [12]. Spreading the data distribution informally among several nodes over the multiple paths shares the network load optimizing the energy constraints of nodes and increases the lifetime of the network. Also multipath routing probably increases the reliability of the network, minimizes overhead caused for transmission of data and the cost for reconstruction of alternate path during link failure and the decreases the transmission delay by sending the data through multiple paths [13]. Overall we can say that multipath routing protocols satisfy most of the requirement to maintain the Quality of Service (QoS) in the network.

Since the information is transmitted over multiple paths, so the threat of attack also increases. Day by day the communication is becoming vulnerable due to increase in attacks significantly. According to the information given in its annual report Computer Emergency Response Team (CERT) states that in India the computer security incidents increased from six incidents to 57,262 incident within the year 1988 and 2016. MANET suffers from many type of attacks such as flooding attack, routing table overflow attack, sleep deprivation, impersonation attack, node isolation attack, black-hole attack, gray-hole attack, worm hole attack, rushing attack, snare attack, Sybil attack, byzantine attack etc.

In this paper, further we will discuss about different types of attack in section 2. In section 3 we reviewed some paper against Black-hole and Gray-hole attacks. In section 4 we proposed a framework for Co-operative Black-hole attack and Gray-hole attack detection and avoidance mechanism. In section 5 we have compared our protocol with the basic AODV routing protocol and experimental results are provided. In section 6 we conclude the paper with some references.

2. Security Attacks in MANET

2.1. Spoofing Attack

In spoofing attack [14] an attacker node masquerades a legitimate node by gaining advantages over its information, i.e. by altering MAC or IP address of it with a legitimate node as depicted in Figure. 1. It behaves to the other nodes as a friendly node and gains an illegitimate advantage. These types of attack pertained as an initial case of most of the attacks and later on they may lead to a specific and sophisticated one.

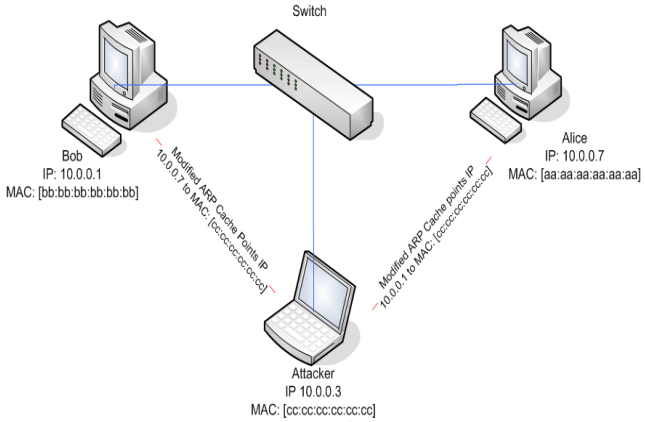

Figure. 1: Spoofing attack.

2.2. Denial of Service attack

Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks [14] are the packet forwarding attacks through which a huge amount of job packets are inserted by the attacker in to the network for creating congestion and contention in the MANET networks.

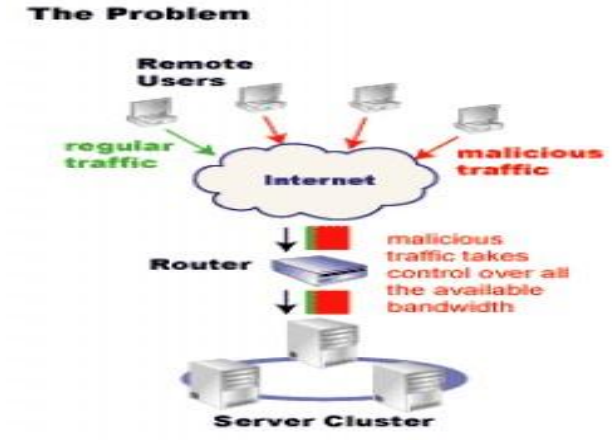

Figure. 2: DOS attack.

Further selective forwarding, routing packets fabrication, routing table poisoning or overflow attacks and SYN flooding may occur which leads into DoS attacks during routing. Overall we can say that DoS or DDoS attacks may be done aiming for different targets but the basic thing to do is to stop the communication for a temporary or indefinite period as depicted in Figure. 2.

2.3. Sinkhole attack

In sinkhole attack [15], an attacker node attracts the network traffic from its neighbor node by using some illegitimate routing information like better routing algorithm, higher bandwidth for communication and shortest path etc. and further after getting all the traffic routed through the sinkhole node, it may drop the routing packets partially or fully leading to DoS. Figure. 3. Represents the sinkhole attack.

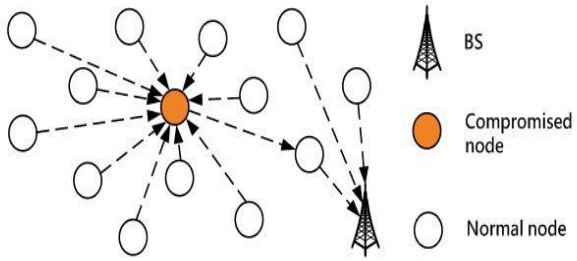

Figure. 3: Sinkhole attack.

2.4. Selective Forwarding Attack

In selective forwarding attack [16], an attacker node applies filtering concept in a particular zone of the network and after getting the filtered traffic, it drops the packets selectively or randomly. This attack becomes more vulnerable when combined with any other types of attack like sinkhole attack. A situation showing a selective forwarding attack is indicated as in Figure. 4.

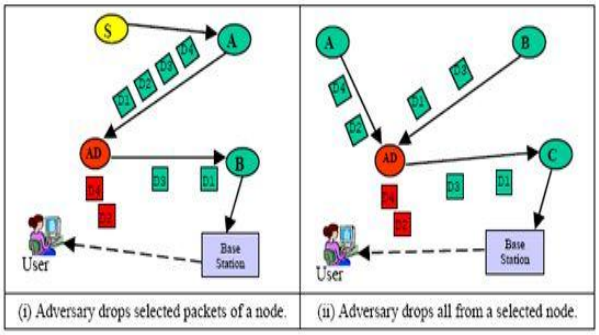

Figure. 4: Selective forwarding attack.

2.5. Sybil Attack

In sybil attack [17] as in Figure. 5, an attacker node handles multiple identities and creates several virtual nodes with new identities using new random or arbitrary identity generation or impersonating or spoofing another legitimate nodes identity to create confusion in routing process or to disrupt the entire network. Sybil attack exploits the property of MANET that it do not have a centralized management system or authority to verify the identities. Sybil attacks are vulnerable to both proactive and reactive routing protocols. In proactive routing protocols an attacker node with a spoofed identity misdirects data to the malicious node where as in reactive routing protocols routing process is disrupted by forming counterfeit identities leading towards DoS.

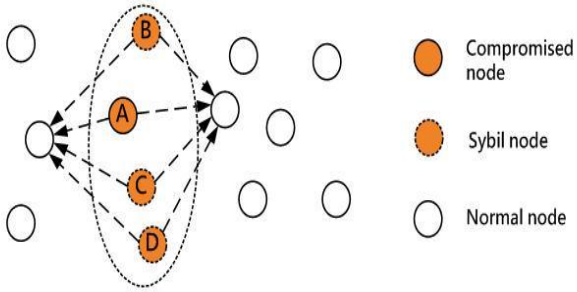

Figure. 5: Sybil attack.

2.6. Wormhole Attack

To exploit the Worm-hole attack [18] successfully, the attacker must have to wait until the node a and b has a connection or exchange the information as shown in Figure. 6.It introduces a malicious node 'X' which is present within the coverage area of the communicating nodes 'a' and 'b'. Intruder creates a tunnel between the a and b and control the traffic between the nodes 'a' and 'b' without affecting the behaviour of the protocol during routing. 'X'

is virtually visible to the entire node which appears as an extraneous node exit between the established links. The 'X' node drop tunnelled packets and break the link. Sometimes it also creates a longer worm-hole link created from 'X' to 'Y'.

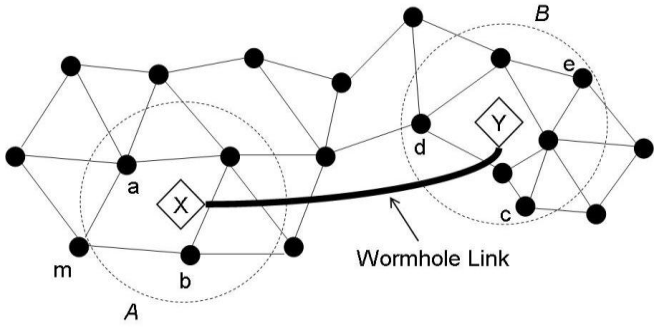

Figure. 6: Wormhole attack.

2.7. Blackhole Attack

In the aim of destroying the the communication by limitising the the communication information flow to other nodes, an attacker drops received routing messages, instead of replaying them.

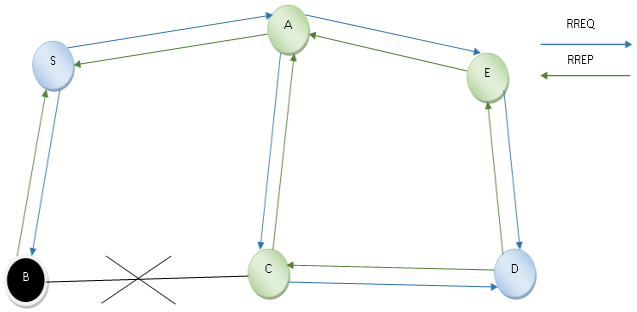

Figure. 7: Black-hole attack.

It's a passive attack which may be extended further to launch DoS(Denial of service). This attack can be launched in bulk or selectively on a node, to the effect of making downgrade communication or the destination node unreachable. Selectively this attack can drop routing packets for a specific node or a portion of packets. In details a black-hole [11] is a malicious node as depicted in Figure. 7, which replies the Route Request (RREQ) in fake without having any route towords the desination and drops all the packets.

2.8. Gray-Hole Attack

Grey-hole [11] attack is special case of black-hole attack in which an attacker becomes the part of an active route within the network as in black-hole attack but does not drop the data packets routed through it entirely. Initially attacker node may behave as legitimate node to trust but later on drop packets selectively with certain probability from some specific nodes or in some other specific pattern. In this type of attack detection of attacker nodes are very difficult as these nodes drop packets routed through them for some time whereas may behave normally as legitimate nodes for the rest of time.

Gray-hole attack may apply through two ways which are given below

i. Dropping all incoming UDP packets.
ii. Partial dropping of UDP packets with random selection process.

3. Literature review

3.1. Defence against Black-Hole Attacks

Tamilsevan et al. [19] suggested a method to prevent Black-hole attack in which a node waits for route replies from several neighbour nodes instead of sending data packets to the reply nodes immediately. They used a Time Expired Table (TET) and collects Route Reply Table (CRRT) for storing sequence number and packet arrival time. From CRRT availability of repeated next-hop node is checked and in case of unavailability random routes are selected.

Lee et al. [20] presented a Black-hole avoidance method using confirmation request (CREQ) and route confirmation reply (CREP). Each intermediate node sends RREP to source node along with the CREQs to the next hop towards destination. Finding a route to the destination similarly an intermediary node sends the CREP to the source. Source node compares the path in RREP and in CREP and finding the identical paths announces the route to be correct. This scheme fails when two colluding consecutive node work together to form a Black-hole attack.

Shurman et al. [21] presented a method based on sharing of hops in Black-hole. Here the source node waits for multiple RREPs and compares them for shared hops and finding a shared hop declares the route as safe. This scheme delivers a time delay of waiting for multiple RREPs.

Kurosowa et al. [22] proposed a Black-hole detection approach which relies that a source can be convinced easily that the path is optimum and that should be chosen for routing purpose, by any node with sufficiently increased destination sequence number. Black-hole attack detected by making the statistical analysis of the difference between the destination sequence numbers of the RREPs received.

TOGBAD [23] is a Black-hole detection mechanism for OLSR proactive routing protocol which uses topology graph for Black-hole detection. According to the graph a node claims the actual number of neighbours looking at the no of neighbours.

Medadian et al. [24] suggested a method to detect Black-hole attack in AODV in which a judgement process is initiated by the receiver node about the sender node after receiving a reply and each of its neighbours share their opinion. Based on a threshold value of the opinions a decision is made. This scheme suffers from high false alarm rate due to dynamic environment of MANET and less adaptability to changes occuring to topology of the network due to mobility of nodes.

Zhang et al. [25] proposed a secure incentive protocol to prevent Black-hole attack which rewards credit charged to nodes for the packets, which means the nodes using resources excessively without any contribution to the network will run out of credit. This scheme opens new possibilities for explanation of the network.

Ketan et al. [26] suggested a Black-hole removal technique for AODV with marginally high processing overhead in which a node receiving two RREPs compares their destination sequence number. Whenever the difference between those two sequence numbers becomes notably high, then the node sending RREP possessing exceptionally high destination sequence numbers is considered as a malicious node. To isolate that suspected node from other nodes in the network an alert message is conveyed throughout the network. This approach fails when a malicious node does not use arbitrary high destination sequence number.

3.2. Defence against Gray-Hole Attacks

Xiaoping et al. [27] proposed a detection mechanism for Gray-hole attacks in DSR routing protocol in which an aggregated signature algorithm, check-up algorithm and a diagnostic algorithm is used by each node to produce the evidence of forwarding packets, checking packets have been dropped or not, to trace the malicious nodes. Aggregate signature algorithm facilitated using a Distributed Certificate Authority (DCA) in with a small change to previous one.

J.Sen et al. [28] suggested a local and co-operative detection mechanism to identify malicious Gray-hole attacks. The procedure consisting of four sub procedures as: neighborhoods data collection, local anomaly detection, co-operative anomaly detection and global alarm raiser procedure by taking care of the collaborating malicious nodes for not declaring legitimate nodes

as malicious. In this protocol the number of RTS (request to send) and CTS (clear to send) messages are checked for making a local detection. Further when a node found to be doubtful, the neighbors of the suspected node collaboratively decide about the node for declaring it malicious.

Dhamade et al. in [29] proposed a Gray-hole minimization technique by using a Request Reply table. Request Reply table is maintained at each node and used for storing all the RREP requests received by it. Further analyzing the RREP entries present and comparing Destination Sequence number with Source Sequence number are malicious nodes are identified and removed. This approach suffers from a high end to end delay as a node has to wait for multiple number of RREP's to arrive until a particular timeout.

Kariya et al. in [30] suggested a Course Based Detection Method for detecting Gray-hole attack in MANET by monitoring only those neighboring nodes that are involved in the route. Source node maintains a Forward Packet Buffer to keep a copy of packets forwarded to the neighboring nodes in the route until the neighboring node forwards it. Source node computes the percentage of packets sent by the neighbor to original packet sent. If this computed value falls below a threshold value fixed before then the neighbor node considered as malicious.

4. Proposed Framework for Co-operative Black-Hole Attack and Gray-Hole Attack

First divide the network into number of zone where each zone consists of one static intelligent node (SIN) and normal nodes. The total network at any time can be connected with the help this intelligent node.

4.1. Terms Associated with Proposed Framework

4.1.1. Zone Splitting (ZS)

The network is divided into number of zones where each zone consists of normal mobile nodes and one Static Intelligent Node (SIN) which is quite reach in resource in comparison to the general mobile nodes.

4.1.2. Node Registration

Initially all the mobile node for the first time communicate with SIN in their corresponding zone. In this communication process, SIN will give a public ID which is used for communication and a private ID which is used for the security check.

4.1.3. Route Request (RREQ)

Whenever a mobile node wants to communicate with another node and the route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ table as described in Table 1 contains the following fields.

Table 1: Contents of route request table

Source Address	Destination Address	Destination Sequence Number	Hop Count	Life Time

4.1.4. Route Reply

When an intermediate node is the destination node or it is having a valid route towards the destination node, then it unicasts a route reply message (RREP) back to the sender as described in Table 2. This message has the following format.

Table 2: Content of route reply table

Source Address	Request ID	Source Sequence Number.	Destination. address	Destination. Sequence Number	Hop Count

The reason one can unicast RREP back is that every node forwarding a RREQ message caches a route back to the source node.

4.1.5. Zone Node Communication (ZNC)

Whenever a normal node want to communicate with another node, and the path with the destination is established then it communicates with the SIN and store the communication information in the database i.e. source node, destination node, number of packet, possible route for transfer of packet etc. The entire process represented pictorially in Figure. 8 and 9.

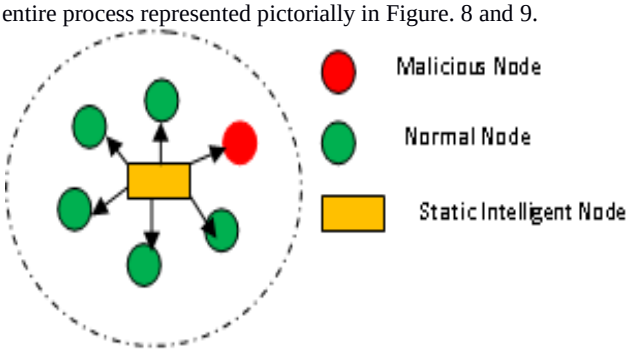

Figure. 8: Request message from SIN to all nodes of the corresponding zone.

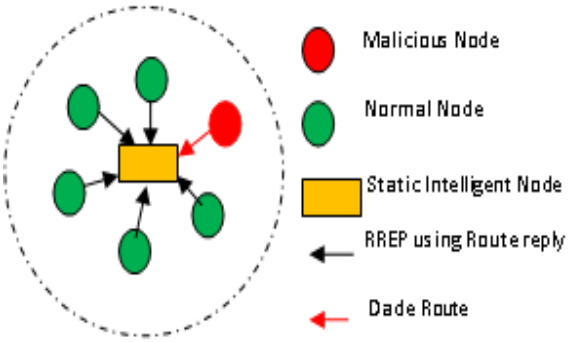

Figure. 9: Route reply from the neighbouring nodes.

4.1.6. Periodic Node Investigation

Periodically, static intelligent node (SIN) sends the request to all the nodes in the corresponding zone. The node must reply back with the help of private ID.

vii. Non periodic node investigation: If a node in a certain zone does not receive some packet, then it will send this information to the static intelligent node of that zone. Then SIN of that zone will communicate with the SIN of the zone through which the packet is transmitted. After receiving a message, SIN of that zone start the process of investigation similar to the periodic node investigation.

4.2. Steps to Detect and Avoid External Malicious Black-Hole and Gray-Hole Node

Step 1: Periodically Static intelligent node (SIN) sends a request to all the nodes present in the zone.

Step 2: After receiving a request from SIN, all the nodes send reply back to SIN.

Step 3: Non-malicious nodes communicate with SIN with the help of Private ID about which the malicious node is not aware.

Step 4: SIN compares the ID received from the node with its own database.

Step 5: If the ID does not match or not present in the database, then corresponding node is malicious.

Step 6: Send a message about the malicious node to all the non-malicious nodes of that zone.

Step 7: In this way, non-malicious nodes of the zone become aware of the malicious nodes.

Step 8: Further all transmissions path through that node is avoided during communication.

4.3. Steps to Detect and Avoid Internal Malicious Black-Hole and Gray-Hole Node

Step 1: Each node monitors its neighbor and stores the information about that neighbor in its neighbor table.
Step 2: A particular node monitoring its neighbor during data transmission if found anything suspicious then records its view about the node in its neighbor table in form of packet drop rate. The views are somehow considered neglecting the packet loss up to some extent as in MANET data transmissions always affected by the factors like limited bandwidth, limited memory, and less amount of CPU cycles and network congestion. But if the data loss is more than the threshold then the monitoring node marks it as suspicious.
Step 3: Getting a node to be malicious the monitoring node shares its view with the SIN.
Step 4: SIN without declaring the node immediately as malicious and taking a step against false detection initiates a detection process for the black hole and gray-hole attacks.
Step 5: SIN sends a trace message to each node present within its zone and ask for a reply with information about the monitoring report of all its neighbors.
Step 6: Getting the replies from every node SIN finds the average of all the views i.e. the packet drop rates and then comparing it with the threshold value, draws an conclusion about the node to be malicious or not.
Step 7: Finding a nodes packet drop rate below threshold declares it as malicious and send a message about the malicious node to all the non-malicious nodes of that zone.
Step 8: In this way, non-malicious nodes of the zone become aware of the malicious nodes.

5. Simulation and Results

We have considered the basic AODV routing protocol to compare with our proposed routing protocol for the performance evaluation. Performance matrices like packet delivery ratio, routing packet loss and network throughput are taken into consideration during evaluation. The basic reason of considering the AODV routing protocol for comparison is that our routing protocol is constructed as a reactive routing protocol by modification in AODV and adding the security features as well as the zone concepts. NS-2.35 simulator is used for simulation study and XGRAPH for plotting the results. Table 3. shows the detailed scenario and parameter setting used for this simulation purpose.

Table 3: Simulation scenario and parameter settings

Parameter Name	Value
Number of nodes	40
Node distribution	Random
Area dimension	1500 x 750
Simulation time	300 s
Propagation	Radio-propagation model (Two way)
Network type	Wireless
Traffic generator	CBR
MAC type	IEEE 802.11
Data rate	11 Mbps
Antenna type	OmniAntenna
Mobility pattern	Random
Interface queue type	DropTail/PriQueue
Max packet in interface queue	50

5.1. Packet Delivery Ratio

Packet delivery ratio is the ratio of number of packets received by the receiver with respect to the number of packets sent by the sender. Figure. 10 shows the comparison between the basic AODV and our proposed routing protocol for the packet deliver ratio metric. From the result we can conclude that our proposed protocol shows a substantial increase in packet delivery ratio over AODV in presence of black-hole attack due to the possible detection and avoidance of black-hole nodes during routing path selection. Also the multipath routing mechanism used in our proposed scheme increases the packet delivery ratio through distribution of routing packets over multiple path increasing efficiency during transmission.

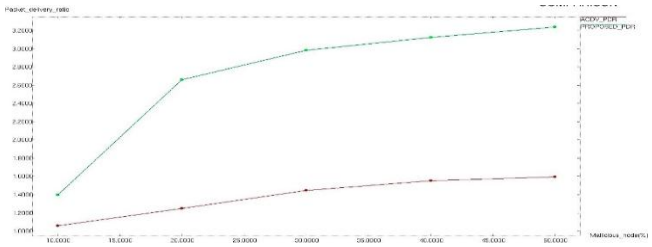

Figure. 10: Comparison graph showing packet delivery ratio.

5.2. Packet Loss

Packet loss during data transfer is exceptionally minimized in our proposed routing protocol in comparison to the basic AODV routing protocol as shown in Figure. 11. This happens as our routing protocol uses multipath scheme to send the packets over multiple path, it decreases the chance of packet loss due to congestion over a single path. The packet loss due to external and internal black-hole nodes also avoided using the private key and neighbour monitoring with voting scheme respectively as proposed.

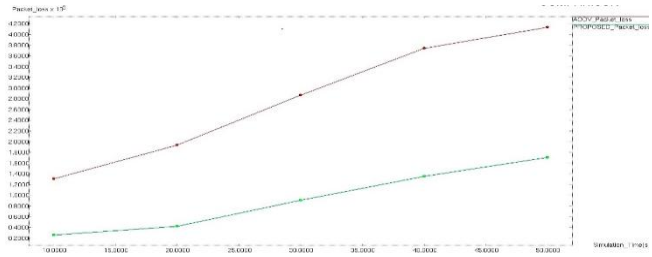

Figure. 11: Comparison graph showing routing packets lost.

5.3. Network Throughput

Network throughput of our proposed scheme observed to be high in comparison to the basic AODV routing protocol as our scheme focuses on optimal path selection along with providing security during communication avoiding partial and full packet drop by malicious nodes, it increases the efficiency and throughput of the entire network. The result showing the comparison of the network throughput metric is given in Figure. 12.

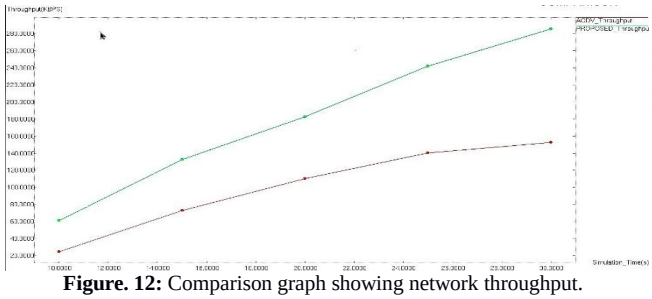

Figure. 12: Comparison graph showing network throughput.

6. Conclusion

In this paper, we elaborate different types of attacks and also proposed a defensive mechanism to Gray-hole and Black-hole attacks in MANET. We introduce a concept of Intelligent Mobile Node, which successfully detects Gray-hole, Black-hole attacks and after detection some action can be taken against those attacks. Our proposed mechanism may require extra cost for implementing Static Intelligent Nodes in a network, but with the help of this method secure packet loss can be minimized and throughput can be increased. We can say that some attacks may lead to cause other attacks and should be given attention separately providing high

degrees of security during routing in MANETs as they are inherently vulnerable to security attacks.

References

[1] Giordano, Silvia. "Mobile ad hoc networks." *Handbook of wireless networks and mobile computing* (2002): 325-346.

[2] Yih-Chun, Hu, and Adrian Perrig. "A survey of secure wireless ad hoc routing." *IEEE Security & Privacy* 2.3 (2004): 28-39.

[3] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[4] Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." *Ad hoc networking* 5 (2001): 139-172.

[5] Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." *ACM SIGCOMM computer communication review*. Vol. 24. No. 4. ACM, 1994.

[6] Chang, Jae-Hwan, and Leandros Tassiulas. "Energy conserving routing in wireless ad-hoc networks." *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. Vol. 1. IEEE, 2000.

[7] Singh, Debabrata, Binod Kumar Pattanayak, and Chandan Kumar Panda. "Analysis of an improved energy balanced routing protocol for wireless sensor network." In Communication and Signal Processing (ICCSP), International Conference on, pp. 1807-1811. IEEE, 2016.

[8] Rath, Mamata, Bibudhendu Pati, Binod Kumar Pattanayak, Chhabi Rani Panigrahi, and Joy Lal Sarkar. "Load balanced routing scheme for MANETs with power and delay optimisation." International Journal of Communication Networks and Distributed Systems 19, no. 4 (2017): 394-405.

[9] Chandel, Jyotika, and Navneet Kaur. "Energy Consumption Optimization using Clustering in Mobile Ad-Hoc Network." *International Journal of Computer Applications* 168.12 (2017).

[10] Deepa, J., and J. Sutha. "A new energy based power aware routing method for MANETs." *Cluster Computing* (2018): 1-8.

[11] Panda, Niranjan, and Binod Kumar Pattanayak. "Energy aware detection and prevention of black hole attack in MANET." *International Journal of Engineering and Technology (UAE)* 7.2.6 (2018): 135-140.

[12] Tarique, Mohammed, et al. "Survey of multipath routing protocols for mobile ad hoc networks." *Journal of Network and Computer Applications* 32.6 (2009): 1125-1143.

[13] Stavrou, Eliana, and Andreas Pitsillides. "A survey on secure multipath routing protocols in WSNs." *Computer Networks* 54.13 (2010): 2215-2238.

[14] Panda Pankajini, Gadnayak Khitish Ku., Panda Niranjan, "MANET Attacks and their Countermeasures: A Survey", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 11, pp. 319 – 330, Nov 2013.

[15] Kim, Gisung, Younggoo Han, and Sehun Kim. "A cooperative-sinkhole detection method for mobile ad hoc networks." *AEU-International Journal of Electronics and Communications* 64.5 (2010): 390-397.

[16] Pathan, Al-Sakib Khan, ed. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[17] Abbas, Sohail, et al. "Lightweight sybil attack detection in manets." *IEEE systems journal* 7.2 (2013): 236-248.

[18] Patel, Anal, Nimisha Patel, and Rajan Patel. "Defending against wormhole attack in MANET." *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*. IEEE, 2015.

[19] Tamilselvan L, Sankaranarayanan V. , "Prevention of blackhole attack in MANET", IEEE 2nd International Conference, pp. 21-21, 2007.

[20] Lee, Seungjoon, Bohyung Han, and Minho Shin. "Robust routing in wireless ad hoc networks." In Parallel Processing Workshops, 2002. Proceedings. International Conference on, pp. 73-78. IEEE, 2002.

[21] Al-Shurman M, Yoo SM, Park S., " Black hole attack in mobile ad hoc networks", In Proceedings of the 42nd annual Southeast regional conference, pp. 96-97, 2004.

[22] Kurosawa S, Nakayama H, Kato N, Jamalipour A, Nemoto Y., "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method", Internation Journal of Network Security, Vol-5(3), pp.338-46, 2007.

[23] Gerhards-Padilla, Elmar, Nils Aschenbruck, Peter Martini, Marko Jahnke, and Jens Tolle. "Detecting black hole attacks in tactical MANETs using topology graphs." In Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on, pp. 1043-1052, IEEE, 2007.

[24] Medadian M, Yektaie MH, Rahmani AM., " Combat with Black Hole Attack in AODV routing protocol in MANET", First IEEE Asian Himalayas International Conference, pp. 1-5, 2009 .

[25] Zhang X, Sekiya Y, Wakahara Y., "Proposal of a method to detect black hole attack in MANET", IEEE International Symposium In Autonomous Decentralized Systems, pp. 1-6, 2009.

[26] Chavda KS, Nimavat AV., " Removal of black hole attack in AODV routing protocol of MANET", IEEE Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1-5, 2013.

[27] Xiaopeng G, Wei C., "A novel gray hole attack detection scheme for mobile ad-hoc networks", NPC Workshops. IFIP International Conference, pp. 209-214, 2007.

[28] Sen, Jaydip, M. Girish Chandra, S. G. Harihara, Harish Reddy, and P. Balamuralidhar. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks." In Information, Communications & Signal Processing, 2007 6th International Conference on, pp. 1-5. IEEE, 2007.

[29] Dhamade CS, Deshmukh HR., "An efficient way to minimize the impact of the grayhole attack in ad hoc network", International Journal of Emerging Technology and Advanced Engineering. Vol-2(2), pp.106-110, 2012.

[30] Kariya DG, Kathole AB, Heda SR., "Detecting black and gray hole attacks in mobile ad hoc network using an adaptive method", International Journal Of Emerging Technology And Advanced Engineering. 2(1), pp.775-80.2012.