Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
8(1), 2020, 01-07

ISSN 2347 – 7393

Original Research Article

PREVENTION MECHANISM OF BLACK HOLE AND JAMMING ATTACK IN MOBILE AD HOC NETWORK

Harsh Pratap Singh[1] and Rashmi Singh[2]

[1]Assistant Professor, Sri Satya Sai University of Technology and Medical Sciences, Sehore, India
[2]MIS Head, Trident Group, Madhya Pradesh, India

Abstract*:* Mobile ad hoc network (MANET) is more susceptible to severe kind of security threats like denial of service attack, black hole attack, jamming attack and Sybil attack because of its dynamic behavior and lack of central administration. In such network any number of nodes can join or leave the network easily. In this paper, focuses on the prevention of black hole and jamming attack which is one of the serious threats. Black hole node advertises itself that it has the shortest route to destination while jamming occurs due to uninterrupted radio waves to put down the transmission between receiver and sender. We propose IDPS (Intrusion Detection and Prevention Scheme) scheme to thwart the black hole node and Distributed monitoring mechanism to choose monitor nodes responsible for identifying channel accessibility. The proposed security scheme is able to handle the jamming attack conditions and resolve the problem of link blockage from jamming. The simulation & analysis of proposed work is performed on NS-2.34 network simulator and it is found that our proposed scheme outperforms in prevention for black hole and identifying the jamming nodes.

Keywords: Black hole attack, Jamming attack, MANET, Network Simulator

Introduction*:* The exclusive uses of computer network for sharing or exchanging our personal information and resources increasing hastily day by day. It is mainly classified into two categories wired and wireless network. The wired network has fixed infrastructure but it has limited range and nodes can take parts in the transmission of the information while in wireless network it does not have predefined infrastructure which means it is infrastructure less and decentralized network.[10] It has dynamic behavior and uses dynamic topology to form the network. In such network node can join or leave as per requirement and each node behaves as router or host it means they can transmit the message by selecting the optimal path. But due its dynamic nature the nodes of

For Correspondence:
singhharshpratap@gmail.com.
Received on: March 2020
Accepted after revision: March 2020
DOI: 10.30876/JOHR.8.1.2020.01-07

the network may get compromised and started to perform misbehaving activities. For transmission of message wireless network uses routing protocols which are classified into three categories: Proactive, Reactive and Hybrid routing protocol. [11] The proactive routing protocol the mobile nodes periodically broadcast the routing information to their neighboring nodes. Examples of proactive protocols are DSDV and OLSR etc. In reactive routing protocol [9] when the node is require for the transmission it can added or leave the network. Examples of such routing protocols are AODV, DSR etc. In this work we use AODV protocol which broadcast RREQ and RREP packet. The RREQ (route request packet) packet is broadcast to each neighboring node to select the path and RREP (route reply) packet is delivering the nodes if they has route to destination. This paper discusses about the black hole and jamming attack on the network. Black hole attack advertises or broadcast that the malicious node has the shortest route to transmit the packet earlier and then it drop the packet. In jamming attack, it occurs due to uninterrupted radio waves to put down the transmission between receiver and sender. The organization of the rest section of the paper is done in this manner:

Section II discusses about the formerly work done by the researcher for the prevention of black hole and jamming attack. In section III present the background of Black hole attack and jamming attack and section IV discuss the proposed scheme for the prevention of such attack. In section V shows the experimental results and its analysis. Last section gives overall conclusion of the paper.

Related work: A lots of work has been in the field of prevention of black hole and jamming attack. In this section some the formerly work done by the various researcher is discussing:

Kaur et al. [1] proposed a scheme for the detection of jams using threshold value. If threshold value goes beyond to some boundary then there anticipate some jam on network. When the jam will perceived then test will be performed on the node which will be generating jam. Node uniqueness will be checked by evaluating the distance and the message of that node will be checked to sense the retransmission and replays. If sequence number will identical than attacker will be detected but if sequence number is unusual message content will be checked. To ensure the reason of retransmissions an supplementary message will be send to destination so that if re-transmissions are due to the network malfunction it can be detected.

Yadav et al.[2] proposed work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high data rate are being generated in the network. Their research work was improving the performance of mobile ad hoc networks under jamming attack by using CTS/RTS integrated approach. The performance of network is measured with respect to the QoS parameters like throughput, and delay. OPNET (Optimized Network Engineering Tool) MODELER 16.0 is used for simulation. The results of simulation demonstrate that the overall performance of network with jamming attack has been increased.

Vanitha et al. [3] proposed a probabilistic misbehavior detection scheme is highly desirable to assure the secure DTN routing as well as the establishment of the trust, among DTN nodes. A zone (routing zone) of a node is used to collect the node information within the range. In this protocol, it cannot achieve the packet delivery ratio, performance and data loss rate. In this paper we are providing the solution against black hole attack which is based on fuzzy rule. Fuzzy rule is used to identify the infected node as well as provide the solution to reduce data loss over network. Fuzzy logic ranges between the value as {0, 1}. Geographic routing is one of the most suitable routing strategies in wireless mobile Ad hoc network mainly due to its scalability. Multi Input Multi Output technique used to send data frequently in routing protocol. Analysis and simulation results demonstrate the effectiveness and efficiency of

the drop node analysis, high packet delivery ratio, throughput and delay.

Kaur et al. [4] proposed a method to design a mechanism of blackhole detection based on artificial neural networks (ANNs). Using a simulated MANET environment, ANNs modeling for detecting the black hole attack is investigated and it is showed that model can detect nodes under blackhole attack effectively.

Wahane et al. [5] proposed the modification of Ad Hoc on Demand Distance Vector Routing Protocol. The proposed work suggests two new concepts, Maintenance of Data Routing Information Table and cross checking of a node. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes.

Mane et al.[6] considered the adversary who is aware of all the specification of protocol which are being used in communication can perform an denial of service attack with the help of jamming the channel used in communication for exchanging the messages. Blocking the radio transmission is called as jamming. The jammer is an entity who intentionally tries to do interference with transmission and reception of messages while the communication is going on. The jammer continuously transmits the radio frequency to fill the channel used in communication so that legitimate traffic will get block. The problem of jamming is being addressed in this work. The attacker is active for short time and will only focus on targeting the data or messages with high importance .this is basically called as targeted jamming. Targeted jamming means jamming only particular part, computer or link. May be the adversary is interested in some specific portion of the victim network and attacking only these portion can proceed to further jamming.

Background for black hole and jamming attack: A black hole attack is one of the Network layer attacks in MANET. It is an attack where one malicious node claims itself as the shortest path to the destination node. Black hole attack can be an internal or an external attack. It can further be classified as:

- Single black hole attack and
- Cooperative black hole attack

Single Black Hole Attack: A single black hole attack is when one malicious node in the network claims itself as the shortest path to reach the destination node. The source node sends the data packet to this malicious node which is either dropped or delayed by the node. There is no interaction among the source and destination nodes regarding the data packet. There can be several ways to detect this attack in the network. One of them is neighborhood based detection method [7][8]. In this scheme, the unconfirmed nodes are identified along with a new routing path from source to destination. It uses lower detection time.

Cooperative Black Hole Attack: The scheme of cooperative black hole is considered when single black hole detection fails. A cooperative black hole is when some malicious nodes collaborate together to behave as the normal route. These nodes hide from the single black hole detection schemes. Several schemes of detecting the cooperative black hole are presented as, DRI table and Cross Checking Scheme, Distributed Cooperative mechanism, Hashed based scheme and Backbone nodes and restricted IP scheme. In the scheme of DRI table and Cross Checking [7] every node maintains a DRI (Data Routing Information) table where bit 1 stands for „true“ and bit 0 stands for „false“. They maintain table of „from“ and „through“ bits on the data packets. In the scheme of cross checking, the source node sends the request message in order to find a secure route for transfer of data packets to the destination node. The intermediate node generates a reply message to the source node which contains information regarding the next hop node with a DRI table entry. The source node checks this entry with its own DRI table to identify it as a reliable node.

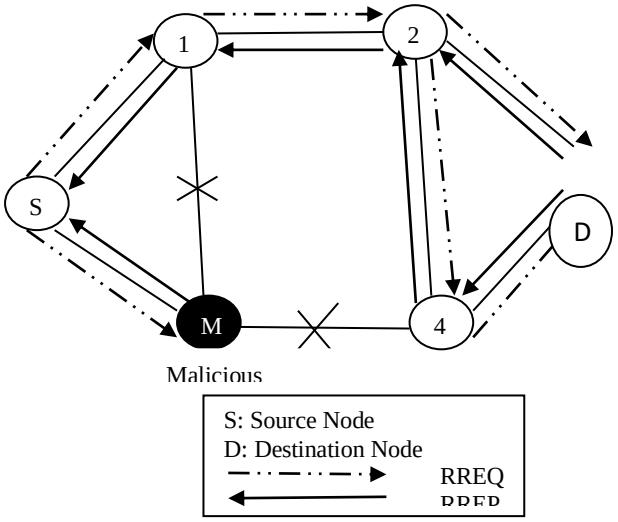

Fig. 1 Blackhole Attack

Jamming Attack: Jamming attack is one of the most popular attack models of IEEE 802.11. Ad-Hoc networks are very prone to security threats. Jamming attack [2] is one of the type of Denial Of Service (DoS). Jamming is caused by continuously sending the radio signals in between the transmission which injects the dummy packets thus causing interferences. Since the radio frequency is an open medium, therefore jamming is big problem for wireless networks. Jamming decreases the overall-performance of network by affecting their throughput, network load, end to end delays etc.

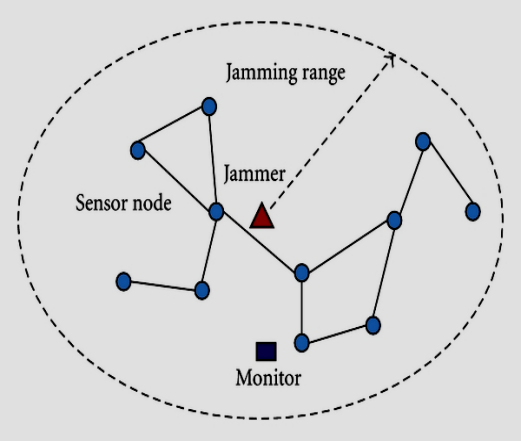

Fig. 2 Jamming Attack

Proposed prevention mechanism: In this section of the work mainly discusses about our proposed scheme for the prevention of black hole and jamming attack over the network.

Blackhole Attack Prevention: As nodes in mobile ad hoc networks have a limited transmission range, they expect their neighbors to relay packets meant for far off destinations. These networks are based on the fundamental assumption that if a node promises to relay a packet, it will relay it and will not cheat. The reputations of the nodes, based on their past history of relaying packets, can be used by their neighbors to ensure that the packet will be relayed by the node. An intrusion detection and prevention scheme (IDPS) to detect and defend against malicious nodes' attacks in MANET is presented here. The IDPS are breaks into two part IDS (intrusion detection system) and IPS (Intrusion Prevention System), IDS are apply for behavior analyzing of the network that time we apply AODV routing protocol and one blackhole attack node, that node mislead at the time of sender broadcast routing packet in the network so black hole node certainly response reply to the sender node and then sender node send's data packet through black hole node without any other information tacking of routed node, that black hole node capture the data packet and can't send that packet to actual receiver node so this type of mislead detect through file processing technique and analyze the network behavior after that scheme in next module we execute that time we create IPS node and IPD provide secure communication on to the network so no any mishappens in the network. All the work done through NS-2 simulator and simulate our result.

Jamming attacks prevention: In this work we will made an important observation that no measurement is sufficient to reliably classify jamming attack. We build our work on the basis of this observation and develop a detection and prevention mechanism that removes the ambiguity in detecting jamming from congested scenarios. In this work, we will focus on detecting jamming attacks that occur at both MAC layers and network layer of an 802.11 ad

hoc network. We present a distributed monitoring mechanism to choose monitor nodes responsible for identifying channel accessibility. The proposed security scheme is able to handle the jamming attack conditions and resolve the problem of link blockage from jamming.

Experimental setup & results: Simulation is a fundamental tool in the development of MANET protocols, because the difficulty to deploy and debug them in real networks. The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems. It offers flexible testing with different topologies, mobility patterns, and several physical and link-layer protocols. However, a simulation cannot provide evidence in real-world scenarios, due to assumptions and simplifications that it makes. Therefore, the results obtained from the simulations should be evaluated appropriately. Three well-known simulators are used for MANET simulations: NS-2.34, GloMoSim and OPNET. We chose NS-2.34, because firstly it is very dynamic and also scalable simulator that is designed especially to large wireless networks. It supports hundreds of nodes, using parallel and distributed environment.

Simulation Environment:

The NS-2.34 Network Simulator [11] is an open-source object-oriented discrete-event simulator for network research. NS-2 provides a framework for simulation of wired and wireless networks, including some facility for emulation. The NS-2 simulator is written in C++ with a Tcl shell in the front end that uses oTcl (object oriented Tcl) libraries. Scenarios are run by feeding an oTcl script to the NS-2 executable. The output can be read directly or post-processed by an interactive graphics viewer called NAM. Generally NS-2 has a different architecture for wireless and wired simulation. Current version of NS-2 does not support any sort of security architecture. So for that purpose special classes were designed

We modeled network traffic using Constant Bit Rate (CBR) sources. A CBR traffic source provides a constant stream of packets throughout the whole simulation, thus further stressing the routing task. In each experiment, half the nodes in the network are CBR sources, and each source transmits 64-byte packets at a rate of 4 per second. We experimented with higher sending rates, packet sizes and number of sources. We omit those results, as they show similar trends, with the predictably higher effect of network congestion.

Table 1 Simulation setup

Simulation used	NS-2.34
Topology area	1000 X 1000
No. of Mobile Nodes	50
Simulation Time	150
Speed	45 m/sec
Packets	CBR
Black hole	1, 2, 3
Protocol	AODV, Black hole AODV, IDS-AODV

Analysis of Results: This figure shows the comparison among different black hole node is done using end to end delay parameter and we found that the delay rapidly increases or decreases in case of black hole node while delay in IDS remain constant at a certain level.

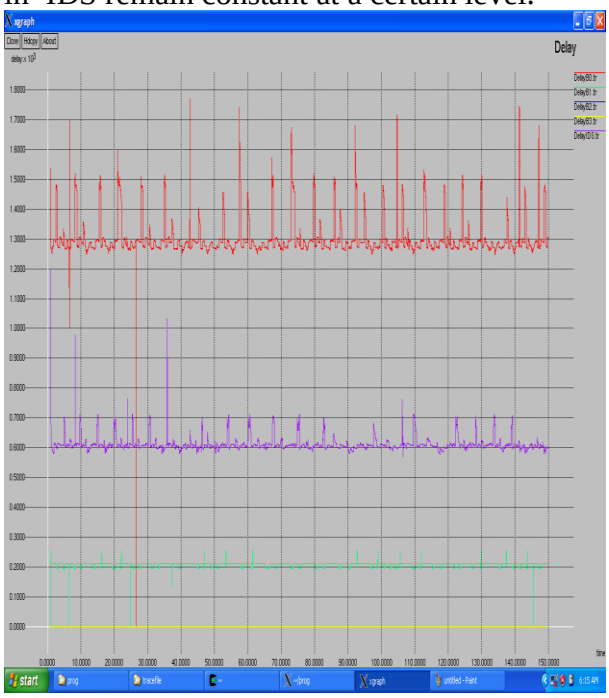

Figure 3 End to End delay comparison among black hole and IDS

This figure 4 shows the comparison among different black hole node is done network routing load and analyzes that the black hole node enhances the network load which degrade the performance of the system in case of black hole node while load due to IDS it maintain the load over the network.

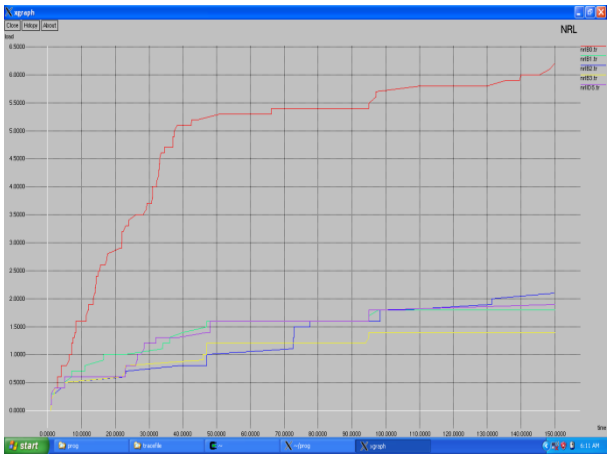

Figure 4 Network Routing Load comparison among black hole and IDS

This figure 5 shows the comparison among different black hole node is packet delivery ratio and analyzes that the black hole node sometime greatly enhance or diminish the PDR due to overhead and loss of packet occurs whereas IDS maintain its PDR at the certain rates.

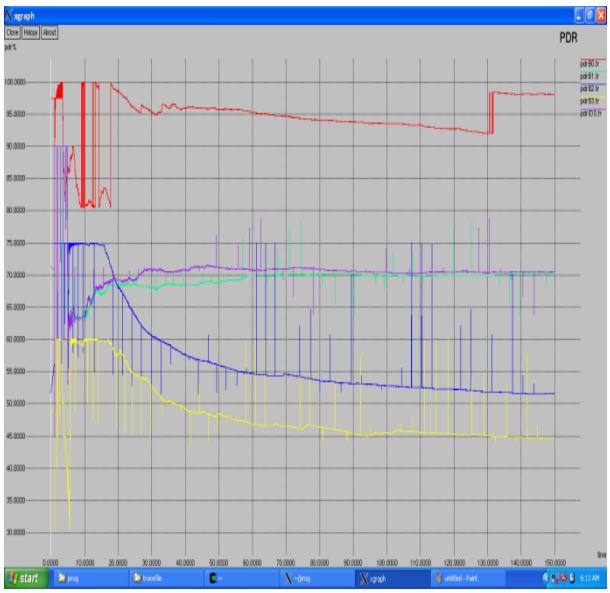

Figure 5 Packet Delivery Ratio comparison among black hole and IDS

This figure 6 shows the comparison among different black hole node is throughput parameter and analyzes that the black hole node sometime throughput becomes more than 100% which is not possible and sometimes its degraded in much amount whereas IDS maintain through put rate approx 85-90 %.

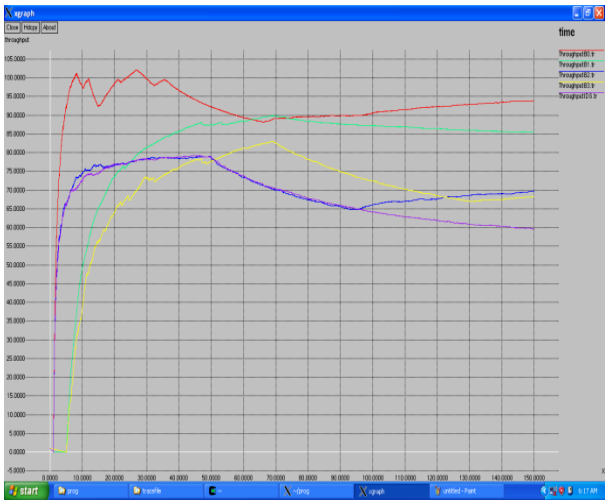

Figure 6 Throughput comparison among black hole and IDS

Conclusion: In Wireless ad hoc network due to its dynamic behavior various kind of attack gets compromised. The jamming attack and black hole attack is one of them. In this work we present the prevention mechanism for both the attack and simulate the work in network simulator NS-2.34. The experimental result of our work outperforms than the existing mechanism.

Reference

[1] Ashwinder Kaur, Abhilash Sharma, "Efficient Detection and Prevention of Jamming Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 129 – No.3, November2015.

[2] Neeti Yadav, Vivek Kumar " Securing Ad hoc Network By Mitigating Jamming Attack", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 6, June 2015.

[3] S. Karthika, N. Vanitha, "Secure Routing Protocol in Delay Tolerant Networks Using Fuzzy Logic Algorithm", International Journal of Advanced Research in Electrical, Electronics

and Instrumentation Engineering, Vol. 4, Issue 5, May 2015, ISSN (Print) : 2320 – 3765.
[4] Ramanpreet Kaur and Anantdeep Kaur "Blackhole Detection In Manets Using Artificial Neural Networks", International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014 ISSN (Online): 2347 – 4718.
[5] G. Wahane, A. Kanthe. S "Techniques for detection of cooperative Black hole Attack in MANET" in IOSR-JCE, 2014.
[6] Ashwini Mane, Rupali Gobe, Poonam Umadikar, Namrata Gawali M. A. Ansari, "Detection and Prevention Jamming
Attack in Wireless Communication", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 886-892.
[7] Mohammad Al-Shurman and Seong-moo yoo and Seungjin park, "Black hole attack in Mobile adhoc networks". AMCSE"04, April 2-3, Huntsville, AL, USA, 2004.
[8] Shrevin Ehrampoosh and Ali Mahani, "Securing Routing Protocol: Affection on MANET"s Performance", International Journal of Communications and Information Technology (IJCIT), Vol.1, No.1, pp.7-15, Dec 2011.
[9] Tseng Y.C., Shen C.C, and Chen W.T. "Mobile IP and ad hoc networks: An integration and implementation experience" Technical report, Department of Computer Sci. and Inf. Eng., Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.
[10] Harsh Pratap Singh, Jitendra Sheetlani, Nagesh Salimath, K Murali Gopal, "Design and Implementation of an Algorithm for Mitigating the Congestion in Mobile Ad Hoc Network", International Journal on Emerging Technologies, 2019, Volume 10, Issue 3, pp 472-479.
[11] Harsh Pratap Singh, Rashmi Singh, "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol", International Conference on Electronics and Communication Systems (ICECS), 2014. In proceeding of IEEExplore, pp. 1-8.