ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 4, April 2015

A Survey on Management of Misbehaving Node in MANET

R.K.Ambedkar[1], Praveen Kumar Joshi[2], Kundan Saun[3]

Sinhgad Institute of Technology, Lonavala, Pune, India[1,2,3]

Abstract: MANET (Mobile Ad-hoc Network) is a dynamically changing network which is self-configuring and used in infrastructure less environment. The nodes in MANET act as router and due to its dynamically changing topology it is more open to attacks that causes network issues and service failures. The malicious node(s) causes dropping of packets are black hole and nodes which are dropping and forwarding only selective packets are called as gray hole which is very difficult to detect as other reasons such as congestion and low bandwidth are also responsible for dropping of packets. So, the security solution must be developed to detect and manage black and gray hole attack. In this paper we attempted to mitigate the black hole and gray hole attack and how these attacks are managed.

Keywords: Mobile Ad-hoc Network (MANET), Cluster, Gray hole attack, AODV.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless nodes in the networks where no infrastructure is provided and have no central control. MANET set up can be done in any previously existing network.

The media that is used for communicating between the nodes in a network is wireless and not reliable. The nodes in MANET are free to move at any position thus forming a dynamic topology and at the same time are acting as router as well. This sort of network is used in many applications such as in disaster relief program, military operations, industrial monitoring and in commercial sector. These networks are exposed to different types of attacks because no central control, nodes are free to leave, join and move inside the network and less resources. The attacks are various types of DoS (Denial of Service) attacks [1] [2]. The attack such as gray hole attack and black hole attack are one of the most important security issues is the safety of network layer.

MANET deals with some major issues such as protocols of routing, security, service discovery, power constraints, mobility management and IP addresses, Quality of Services (QoS), etc. [3].

Techniques used to improve the security of an ad- hoc network. are expensive to implement. MANET has many security issues. Various services such as privacy, network services and reliability are obtained by assuring that security issues have been met. As MANET have dynamic topology so it is more prone to security issues. Thus beside the security threats in MANET factors have changed the conflict zone situation. [4]

In this paper we tackled two types of routing attacks namely Gray hole attack and Black hole attack which exhibits packet forwarding misbehaviour.

The malicious node (black hole) provides implication to other nodes in a network that it follows an efficient path and as soon as the packet is forwarded to this node it straight away drops those packets. In gray hole attack, the malicious node (gray hole) do not drops all the packets which are forwarded to it and this behaviour of Gray hole node makes it difficult to detect. However, both attacks are mainly targeted on route discovery process disturbance and degrading network’s performance.

1.1. Black Hole Attack

Black hole attack is a type of DoS attack. The black hole node gives implication to other nodes that shortest path to the destination is through it but in reality it is not the case. The source believes and sends the data packet through this black hole node and as soon as the packet is received at the black hole node it drops the packet and network performance is hampered.

1.2. Gray Hole Attack

Gray hole is the variation of Black hole attack. Gray hole attack has uncertain behaviour as sometimes it forwards the packet and sometimes packet is dropped. So it becomes a tough task to detect the malicious node as the packet lost at the destination node may be caused due to other reasons such as congestion etc. This uncertain behaviour makes it difficult to get detected.

II. VARIATIONS OF GRAY HOLE ATTACK

The gray hole attack is understood in two parts. Firstly, the gray hole node exploits AODV (Ad-Hoc on Demand Distance Vector) protocol. The packets are interrupted and false implications are passed on to the source about the route [5].

And then it drops the interrupted packets. The gray hole node advertises itself using a routing protocol that it has shorter pathway to the destination node. During the route discovery process, the gray hole node promotes that availability of fresh and shortest path despite looking into their routing table entries. So a forged path is created through responses received from the malicious node to the source nodes. After the route is created Gray hole node will decide to drop data packets or forward to the unknown node (address).

DOI 10.17148/IARJSET.2015.2417

2.1 Active attack

Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of the network in such case the active attack act as an internal node in the network. Being an active part of the network it is easy for the node to make use of and take over any internal node to use it to introduce a false packets injection or denial of service. Figure 2 shows active and passive attack

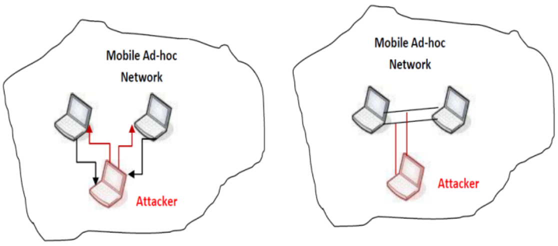


Figure 2 Active and passive gray hole attack

2.2 Passive attack

In passive attack, it listens to the network in order to know and understand how they are located in the network, how the nodes are communicating with each other. Before the attacker starts an attack against the network, the attacker has enough information about the network that it can easily capture and introduce attack in the network.

The AODV protocol is prone to the various malicious attacks such as black hole and gray hole attack. A gray hole node replies positively with a RREP message to every RREQ; but it does not contain a legal route to destination node. As in gray hole node routing table is not necessarily checked RREQ is responded most of the time. Thus source node forwards data through this malicious node, which drops the received packets which are supposed to be forwarded to the destination. So a malicious node can easily divert a lot of network traffic to itself and could cause an attack to the network. Researchers have proposed solutions for identification and elimination gray hole nodes.

S. Banarji et. al. [6] Proposed an algorithm in which before starting the communication source node sends prelude message to the destination the message contain source address, destination address and no. of data packets to be sent.The neighboring node monitors the data traffic and checking whether the next node forward the all data packets or not. At the receiving end after the message is received node sent a postlude message within expire time the message contain no. of data packet received if a data packet received is out of acceptable range then the process of detecting and removing malicious nodes is started by collecting response from the neighbouring node. In this algorithm the overhead is increasing due to additional routing packets. When source node detects black hole node then it broadcasts.

P. Agrawal et. al. [7] In this technique backbone network of strong nodes are established over on an ad - hoc network. In which it assumes that each node in the network is a strong node and trustful node but if it acts as a malicious node then it is detected as a regular node in the network. Source node, send every data block after sending data block it ask the backbone network to carry out end-end checks to destination, whether data packet reached to destination or not.

If the data packet never received at destination or destination aware about any kind of attack then it would inform the backbone network. Following this the backbone network starts the detection of the chain of malicious nodes that are cooperating together to drop the packets.

On receiving a chain message strong node connected with the destination node initialize a list of gray hole chain to contain the id of the node replied to RREQ. It then initiates all the neighbouring nodes to vote for the next node to which it is forwarding packets. If the next id is null then the node is Black hole node. Then the gray hole removal process is stopped and the broadcast to alert the other node in the network. The algorithm will fail if the intruder attacks strong nodes because it violates the assumption that strong node are trusted node.

G. Xiaopang et.al. [8] This technique consists of three algorithms

1. Proof algorithm: - which is based on receiving message source is creating proof of the aggregation signature algorithm.
2. Check up algorithm: - when source are suspect for malicious node then check up algorithm is used.
3. Diagnosis algorithm: -the check up algorithm getting the evidence for diagnosis algorithm for finding the malicious node.

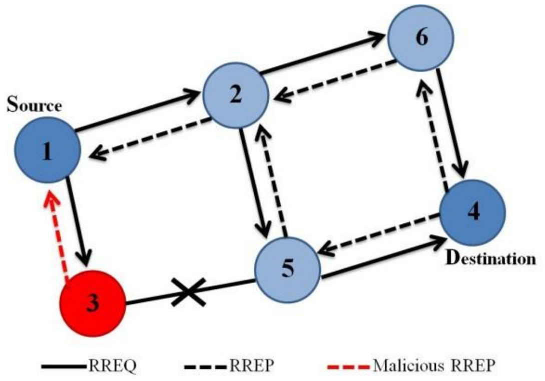
A. Kanthe et. al. [9] Proposed Algorithm in which checks False_Reply_Count is greater than False_Reply_threshold if it is true then it black list the node. In this method, it stops the detection if the routing table sequence number is less than reply packet sequence number. Also it adds a false reply count if the peak value is greater than route reply packet number. This method uses the static value for the detection of gray hole node.

III. PROPOSED AND IMPLEMENTED APPROACH

The proposed and implemented uses a unique and vigorous methodology to detect gray hole nodes. The implemented algorithm is based on AODV protocol which is modified by using crediting and is called CBAODV. This approach is followed in following manner as each and every node assigns a fixed value for its every neighbour node as the neighbour credit value.

This credit value is incremented by when a route request packet (RREQ) is received and decremented when the route reply (RREP) packet is received. When a negative credit value is obtained it is identified as Gray hole node and removes all existing paths from its routing table.

DOI 10.17148/IARJSET.2015.2417



IV. PERFORMANCE METRICS

To evaluate the performance of our solution, we compare our solution (CBAODV) with AODV without attack and AODV with the attack. We consider several performance metrics.

Throughput Ratio

The throughput is defined as the number of bytes received over transmitted per second.

Packet loss Ratio

Packet loss in MANET is complicated because wireless link are subject to transmission error and network topology changes dynamically. A packet may lose due to transmission error, no route to destination, broken link and congestion.

Average end-to-end delay

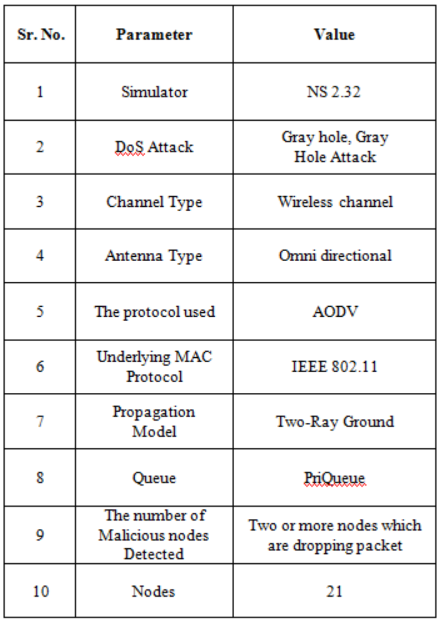
End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

Packet delivery ratio

It is the ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to destination.

∑ Number of packets receive/∑ Number of packet send

V. SIMULATION SETTINGS AND RESULTS



Sr. No.	Parameter	Value
1	Simulator	NS 2.32
2	DoS Attack	Gray hole, Gray Hole Attack
3	Channel Type	Wireless channel
4	Antenna Type	Omni directional
5	The protocol used	AODV
6	Underlying MAC Protocol	IEEE 802.11
7	Propagation Model	Two-Ray Ground
8	Queue	PriQueue
9	The number of Malicious nodes Detected	Two or more nodes which are dropping packet
10	Nodes	21

VI. CONCLUSION

The gray hole attack is one of the serious attacks on MANET. In proposing dynamic AODV approach, we are preventing other clusters in MANET. Our proposed solution simulated using the NS2 simulator and compared its performance with the original static CAODV without attack and with attack in terms of throughput, packet loss rate, packet delivery ratio and end-to-end delay. Simulation results show that once a malicious or misbehaving node is detected in one of the clusters of the MANET it takes minimum efforts to get detected in other clusters. This paper presents good performance in terms of better throughput and minimum packet loss percentage over static CBAODV without attack and static CBAODV with attack.

REFERENCES

[1]. R. Prasad, S .Dixit, R. Van Nee, "Globalization of Mobile and Wireless Communication", March 2011, Springer. ISBN13:9789400701083..

[2]. L. Gavrilovska, R. Prasad," Ad Hoc Networking Towards Seamless Communications", Springer 2006, ISBN: 1402050658.

[3]. A. Kanthe, D. Simunic, M. Djurek , "Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks", MIPRO 2012, IEEE Conference, Proceedings of the 35th International Convention, ISBN:978-1-4673-2511- 6,May21-25,2012, Opatija,Croatia.

[4]. A. Kanthe, D. Simunic , R. Prasad, "Effects of Malicious Attacks in Mobile Ad-hoc Networks", 2012 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India.

[5]. M. Kumar, R. Mishra, "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3. No 1. Feb-Mar 2012.

[6]. S. Banerjee "Detection/removal of cooperative black and gray hole attack in mobile ad hoc networks", In Proceedings of the World Congress on Engineering and Computer Science, October 22 - 24, 2008, San Francisco, USA

[7]. P. Agrawal, R. Ghosh, S. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008

[8]. G. Xiaopang, C. Wei, "A novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" Network and Parallel Computing Workshops, 2007, NPC Workshops, 2007, IFIP International IEEE Conference.

[9]. A. Kanthe, D. Simunic, R. Prasad ," " A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks "International Journal of Computer Application (0975- 8887) Volume 53-No.16, September 2012.

[10]. The network simulator-ns 2.35 http://www.isi.edu/nsnam/ns/, 1996-97

DOI 10.17148/IARJSET.2015.2417