ISSN 2319 - 6629
Volume 8, No.3, April - May 2019
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt03832019.pdf
https://doi.org/10.30534/ijwcnt/2019/03832019

Detection Mechanisms for Gray-hole Attacks in MANET and their Limitations to Overcome Smart Gray-hole Attack : A Review

Nayana Elizabeth[1], Sijo Cherian[2], Aifa S.[3]
[1]PG Scholar, Saintgits College of Engineering, India, nayanandrews@gmail.com
[2]Assistant Professor, Saintgits College of Engineering, India, sijo.cherian@saintgits.org
[3]PG Scholar, Saintgits College of Engineering, India, aifasalih26@gmail.com

ABSTRACT

Nowadays wireless networks tends to be more popular compared to wired networks due to its mobility and scalability. Among the different types of wireless networks, MANET (Mobile Ad-hoc NETwork) is one of the most popular and unique applications. Due to its dynamic network topology each node is free to move around the network. In MANET every node can act as both a transmitter and a receiver. Nodes in this network can directly transmit messages with each other if they are within the same communication range otherwise they rely upon their neighbors for communication. Due to the self-configuring nature of MANET it can be applied in areas like military use, emergency recovery and so on. In MANET it's assumed that all nodes are intimate nodes but in actual scenario some of the nodes become malicious and perform selective packet dropping rather forwarding the data packets. Such type of attack can be generally termed as Gray-hole attack. Among the contemporary grayhole attacks, Smart gray-hole attack is considered to be the most difficult to detect in the network. A smart gray-hole node is a malicious node which acts normally during the route discovery process and after a certain period of time they start dropping data packets routed through them. This type of attacks can severely affect the performance of the network. Hence we require some detection and prevention mechanism against these type of attacks which is considered to be a major issue in MANET. In this paper we discuss about some of the existing mechanisms used to detect gray-hole attacks in MANET and their limitations to overcome smart gray-hole attack.

Key words : G-IDS**,** Intrusion Detection System, MANET, Smart gray-hole attack.

1. INTRODUCTION

Mobile ad hoc network (MANET) is an infrastructure less network which is realized as one of the most progressing and prevalent technology in wireless network. It is scalable, temporary and self-configurable type of networks [1]. MANETs are appropriate for critical operations such as emergency rescue operation, battlefield etc. where the infrastructure based network is hard to set up. Nowadays industrial remote access and control through wireless networks tends to be more popular [2]. Wireless networks allows data communication among different nodes and still maintain their mobility which is one of the main advantage of it. However, this communication is restricted to the range of transmitters. That means when two nodes are beyond their communication range then they cannot communicate with each other so the nodes rely upon their neighbours for transferring messages. For achieving this, mobile ad-hoc networks can be categorized into two, namely, single-hop and multi-hop. In single-hop network, all nodes directly communicate with each other since they are within same communication range where as in a multi-hop network nodes are not within same communication range so they rely upon their neighbour nodes for transferring messages. Fast deployment and minimal configuration make MANET to be used in areas where there is less or no wireless infrastructure support. In MANET, every node act as both a host and a router[3]. These networks comprises of different routing protocols such as AODV (Ad-hoc On-demand Distance Vector) [4], DSR (Dynamic Source Routing) [5] etc. Routing protocols are used for communication and they are based on suspicion that all nodes in the network are intimate nodes but in actual scenario these protocols are sensitive to various types of network attacks, particularly packet dropping attack. Packet dropping attack can be categorized into two, namely, Full packet drop and Partial packet drop. In the case of full packet drop attack or black hole attack, the malicious node gives false routing information saying that it has a valid route to the destination and then drops all the data packets received where as in partial packet drop attack or gray-hole attack, the malicious node performs selective packet dropping attack. Smart gray-hole attack is a type of gray-hole attack in which the malicious node acts normally during route discovery process and afterwards selectively drop data packets. Smart gray attack is hard to detect and has a greater effect on the network performance. For dealing these type of attacks, there is need to provide security in ad-hoc network.

2. LITERATURE SURVEY

The authors Sergio Marti, T.J. Giuli, Kevin Lai [6], and Mary Baker proposed a watchdog scheme which identifies the existence of malicious node in the network by listening to the transmission of its neighbour nodes. This scheme ensures that the packet is forwarded to the next node. When a watchdog node identifies that its neighbour node doesn't forward the packet within a certain period of time, it increments its failure counter. If a node's failure counter outpace a predefined threshold value, then the watchdog node address it as a malicious node.

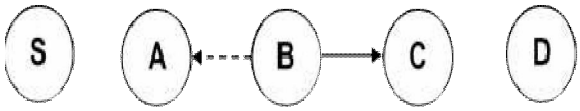

Figure 1: Watchdog scheme: Node B needs to send a packet to node C, the transmission is overhead by node A [6]

The above approach has the following limitations:

- False misbehaviour report.
- Receiver Collision
- Limited Transmission power
- Collusion
- Partial packet dropping
- Hard to detect smart gray-hole attack

The author Sukla Banerjee [7] handled two types of malicious attacks namely, gray-hole attack and black hole attack. In a gray-hole attack the malicious node acts normally during route discovery process and after a certain period of time it drops some or all of the data packets. Gray-hole attack can be categorized into two, mainly sequence number based gray-hole attack and smart gray-hole attack. . Sequence number based gray-hole attack is similar to black hole attack but here the nodes drops the data packets selectively where as in a smart gray-hole attack the nodes acts normally during route discovery process and afterwards drops data packets selectively. A gray-hole attack is a diversification of black hole attack and it's hard to detect. In a black hole attack the node gives false route reply saying that it has the shortest route to the destination and then drops the data packets completely sent to it. In order to tackle these two types of attacks the authors proposed a mechanism in which initially the total data traffic is divided into small sized blocks by the source node. Before sending any block, source node alert the destination node about the incoming data block by sending a prelude message. At the end of the transmission the destination node acknowledges the source node through a postlude message which contains the number of packets received by the destination node. This information is used by the source node to verify whether the data loss is within acceptable range during transmission. If the data loss is not within acceptable range then the source node identifies the presence of malicious node and it will be removed by collecting the response from the monitoring nodes. The above approach has the following limitations:

- High routing overhead due to various extra control packets.
- Hard to detect smart gray-hole attack.

The authors Su, M. Y. [8] introduced some special nodes called as IDS (Intrusion Detection System) nodes which have the ability to listen their neighbouring node's transmission. In this method, the intermediate nodes are not allowed to send the reply packet, only the destination nodes can send the reply packet on receiving the request packet. Here the nodes are declared as malicious based on some rules. The IDS node increments the suspicious value of its neighbour node based on the abnormal difference between requests (RREQs) and replies (RREPs) packets transmitted from the node. If an intermediate node (not the destination node) has never broadcasted a request packet but forwarded a reply packet for a specific path, then its nearby IDS node will increment its suspicious value by 1. If the suspicious value of a node becomes greater than a predefined threshold value then the IDS node isolate it from the network by broadcasting a block message to all nodes in the network about the suspicious node. The above approach has the following limitation:

- Although this approach is able to detect sequence number based gray-hole attack and black hole attack in the network it fails under smart gray-hole attack.

The authors M. Mohanapriya, Ilango Krishnamurthi [9] proposed a new technique for reducing the effects of gray-hole node by introducing some special nodes called as IDSs (Intrusion Detection Systems) in the network. Here the source node says the destination node about the number of packets forwarded by it through the path. When the destination node doesn't get the exact number of data packets, it then transmits a QRREQ (Query Route Request) packet to the node which is at a hop distance of 2 away from it. The destination node then waits for the QRREP (Query Route Reply) packet. The QRREP packet holds data about the number of packets that the node forward to its next hop neighbour node in the source route. The destination node on receiving the QRREP packet, checks whether its previous hop node has sent all the data packets that it received from its previous hop node. If the destination node identifies that its previous hop node doesn't forwarded all the data packets that it received from its previous hop node, the destination node mark it as suspected node and alert to its nearby IDS nodes in the network about the suspected node. The IDS node listens the transmission of the malicious node and whenever it detects an anomaly a block message is broadcasted in the network about the identity of the malicious node and it will be then isolated from the network. The above approach has the following limitation:

- After receiving the query packet, the malicious node can act normally and can forward the data packets due to which the IDS node is unable to detect it.

The authors Rutvij H. Jhaveri, Narendra M. Patel [10] proposed an approach which is based on sequence number threshold that reduces the effect of gray-hole attack in AODV based network. This scheme adds two new fields in the routing table which are node status and last reply time. Node status indicates whether the node is malicious or not. The last reply time indicates the time at which the last route reply for the destination node that updated its sequence number is received. A node receiving the RREP packet identifies that a node sending RREP packet as a suspicious node if the difference between the destination sequence number in the route reply packet and that of the routing table is greater than a particular threshold value. If so a bait request packet is sent to the suspicious node with a non-existing destination address and destination sequence number. The suspicious node is then detected as malicious node if it replies to the bait request and in future the nodes discards all route reply packets from it. The above approach has the following limitation:

- It cannot mitigates the smart gray-hole attack which participates genuinely in the network during route discovery process and sends correct information in the reply packet received either from the destination or any other intermediate node.

The authors Jaydip Sen, M. Girish Chandra, Harihara S.G. [11], Harish Reddy, P. Balamuralidhar proposed a new distributed and cooperative mechanism which comprises of four modules for dealing with gray-hole attack. The modules are:-

- Neighbourhood data collection

In the network each node collects the data forwarding information of its neighbourhood and it will be stored in a DRI (Data Routing Information) table.

- Local anomaly detection module

This module is invoked whenever a node detects a suspicious

node by checking its DRI table.

• The cooperative anomaly detection

This module is invoked to reduce the probability of false detection of the local anomaly detection procedure and thereby increasing the detection reliability.

• Global alarm raising module

Once the gray-hole node has been detected by the cooperative anomaly detection procedure, the global alarm raising module is invoked for sending alarm messages to all nodes in the network about the identity of the gray-hole node. The identified malicious node is then isolated from the network. The above approach has the following limitations:

• Simple gray-hole node is launched by using false route reply but the smart gray-hole node does not send false route reply and behaves normally during route discovery and drops selective data packets.

• DRI based scheme fails under the smart gray-hole attack.

The authors Shashi Gurung, Siddhartha Chauhan [12] introduced a new approach called as Mitigating Gray-hole Attack Mechanism (MGAM), in which some special nodes called G-IDS (Gray-hole Intrusion Detection System) are deployed for detecting the malicious node (smart gray-hole node). These G-IDS nodes are set in promiscuous mode and they can overhear the transmission of their neighbouring nodes. They calculate the number of packets dropped by a particular node and if the value is greater than a particular threshold value, an ALERT message is broadcasted in to the network about the identity of the smart gray-hole node. The smart gray-hole node is then isolated from the network. The above approach has the following limitations:

• G-IDS nodes must be placed such that they should cover most of the simulation area.

• The ALERT message is vulnerable to spoofing attack.

Table 1: Comparative study of existing detection mechanisms

Detection Scheme	**Approach**	**Detection of smart gray-hole attack**	**Overhead**
Watchdog scheme	Using watchdog timer, malicious node can be detected	No	No
Mechanism for detection of gray-hole attack	Data collection, local anomaly, cooperative anomaly, global alarm	No	DRI scheme
Cooperative black hole and gray-hole detection	Prelude message, postlude message	No	Control packets
IDS for black hole attack	Node which never broadcasted RREQ but forwarded RREP for a specific path is detected as malicious	No	Alarm packets
Modified DSR protocol for detection	QRREQ, QRREP	No	QRREQ, QRREP Alarm packets
Bait detection scheme to thwart gray-hole attack	A bait request containing ID of fake node is send to the suspicious node	No	Bait scheme
Novel approach for mitigating gray-hole attack	Malicious node identification by calculating difference between numberof packets forwarded and received by the node	Yes	Alert packets

4. CONCLUSION

In a Mobile Ad-hoc NETwork (MANET), it is assumed that each nodes are trusted nodes. But in actual scenario, there are some nodes that do not participate genuinely in packet forwarding and performs selective packet drop attack which is known as gray-hole attack. Smart gray-hole attack is a type of gray-hole attack which is hard to detect in the network since they act normally during the route discovery process. Security mechanisms plays a vital role in MANET for dealing with these type of attacks. In this paper we have studied various methods that attempt to detect gray-hole attack and their limitations to overcome smart gray-hole attack.

5. FUTURE WORK

Though the Novel approach proposed by Shashi Gurung, Siddhartha Chauhan [12] solves smart gray-hole attack, the limitation regarding the alarm message can breach the network security. Some enhanced intrusion detection system is required to solve the above problem. As a future work, we are planning to tackle this problem by introducing a new approach called asMitigating Smart Gray-hole Attack using enhanced G-IDS (Gray-hole Intrusion Detection System) in which the alarm messages are digitally signed by the G-IDS node using its private key and flooded across the network. A faulty list is maintained to add the malicious nodes detected in the network.

REFERENCES

1. Murthy, C. S. R., & Manoj, B. S. **Ad hoc wireless networks: Architectures and protocols**, Prentice Hall PTR, 2004.
2. Y. Kim. **Remote sensing and control of an irrigation system using a distributed wireless sensor network**, *IEEETrans.Instrum.Meas.*,vol.57, number 7, pp. 1379–1387, Jul. 2008.
   https://doi.org/10.1109/TIM.2008.917198
3. Deng, H. M., Li, W., & Agrawal, D. P. **Routing security in wireless ad hoc networks**, *IEEE Communication Magazine*, 40(10), 70–75, 2002.
   https://doi.org/10.1109/MCOM.2002.1039859
4. Perkins, C. E., Beliding-Royer, E., & Das, S. (2004), **Ad hoc on demand distance vector (AODV) routing**, IETF Internet Draft, MANET working group, 2004.
   https://doi.org/10.17487/rfc3561
5. Johnson, D. B., Maltz, D. A., & Hu, Y-C. (2004), **The dynamic source routing protocol for mobile ad-hoc network (DSR)**, IETF Internet Draft.
6. S. Marti, T. J. Giuli, K. Lai, and M. Baker. **Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks**, *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, Boston, Massachusetts, United States, 2000,255-265.
   https://doi.org/10.1145/345910.345955
7. Banerjee, S. (2008). **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*, WCECS, October 22–24, SanFrancisco, USA.
8. Su, M. Y. **Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems**, *Elsevier Computer Communication*, 2011.
   https://doi.org/10.1016/j.comcom.2010.08.007
9. Mohanapriya, M., & Krishnamurthi, I. **Modified DSR protocol for detection and removal of selective black hole attack in MANET**, *Elsevier Computers and Electrical Engineering*, 40, 530–538, 2014.
   https://doi.org/10.1016/j.compeleceng.2013.06.001
10. Jhaveri, R. H., & Patel, N. M. **A sequence number based bait detection scheme to thwart gray-hole attack in mobile ad hoc networks**, *Springer Wireless Network*, 21, 2781–2798, 2015.
    https://doi.org/10.1007/s11276-015-0945-9
11. Sen, J., Chandra, M. G., Reddy, H., & Balamuralidhar, P. **A mechanism for detection of gray-hole attack in mobile ad hoc network**, *In Proceedings of the IEEE ICICS*, 2007
    https://doi.org/10.1109/ICICS.2007.4449664
12. Shashi Gurung, Siddhartha Chauhan. **A novel approach for mitigating gray-hole attack in MANET**, *Springer Wireless Network*, 24, 565
    https://doi.org/10.1007/s11276-016-1353-5