An Adaptive Identification and Prediction of Attacks in MANET: A Survey

P.Rathiga

Research Scholar, Dept of Computer Science, Erode Arts and Science College, Erode - 638 009
rathigaphd@gmail.com

Abstract

Backgrounds/Objectives: The main objective of this methodology is to reduce the packet loss in intermediate nodes by eliminating malicious nodes in the routing path. Causing packet drop due to attacks by malicious nodes is one of the most significant troubles in MANETs.
Methods/Statistical analysis: In Grayhole and Blackhole attack, the malicious nodes are deliberately disrupting data transmission in the network by sending incorrect routing information. It is a challenge to keep the communication route free from such attackers. The research is conducted to find the most considerable methodology that can detect the malicious nodes without degradation of network performance.
Findings: The various research works has been analysed and its performance is evaluated in terms of packet delivery ratio and End To End delay.
Application/Improvements: The findings of this work prove that the intrusion detection and adaptive response (IDAR) mechanism achieves better results than the other approaches in terms of packet delivery ratio and End To End delay.

***Keywords*:** Black hole attack; Grayhole attack, MANET, malicious node

1. Introduction

In an ad-hoc network, each nodes moves independently which are exchange their information with others using multihop wireless links [1]. Each node in the network acts as a router and forwarding the data packets to other nodes. Due to the node movement, topology of the network is varying dynamically which implement the great challenges to the security of Mobile Ad Hoc Network. As a result, attacker can get benefits of defect in routing protocols to carry out a variety of attacks. The two main attacks such as black hole attack and Grayhole attacks are conventional attacks under Ad Hoc network. These attacks could disturb the routing process or routing protocol and causes lots of damage to the network's topology.

A Blackhole attack disturbs the routing protocol by misleading other nodes about the routing information [2]. The black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the received packets [3]. Grayhole attack is a one of the packet dropping attack. It may occur due to the malicious nodes. In Grayhole attack, a malicious node sometimes acts as a normal node and passes the packets without any damage or dropping. But sometimes same node acts as a malicious node and start dropping the packets. Due to this nature of the malicious node it becomes very hard to detect the Grayhole attack.

In order to reduce the packet drop, various detection mechanisms are implemented in the AODV and DSR protocols [4]. The detection and prevention methods are used to improve the packet transmission process in the correct routing path. The detection mechanism is able to mitigate the foresaid problem by introducing new conditions in the routing table update process and also by adding simple malicious node detection and isolation process to the AODV route discovery mechanism. The proposed method does not introduce any additional control message and moreover, it does not change the existing protocol scheme.

To achieve efficient packet transmission, the Secure Dynamic Source Routing Protocol (SDSR) is introduced to detect and prevent Grayhole attack. When any anomaly is detected, the nearby intrusion detection node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network.

2. Analysis of research methodologies

In [5] introduced a new Mechanism for Detection of Black Hole Attack. In Mobile adhoc network security is important constraints due to their feature of open medium. A variety of protocols exposed various types of attacks. Ad hoc on-demand distance vector routing (AODV) is one of the popular routing algorithms. However, it is vulnerable to the well-known black hole attack, where a malicious node falsely advertises good paths to a destination node during the route discovery process. To overcome this problem defense mechanism is presented against a multiple black hole nodes in a MANET. An introduced defence mechanism efficiently identifies the Blackhole attack and gives the solution to discover a safe route by avoiding black hole attack [2]. According to the proposed solution the required security in MANET can be achieved with minimum delay and control overhead. The defense mechanism dynamically detects the Black hole attack and transmits DATA packets to the destination. However network performance improvement is still investigated.

In [6] proposed a Novel Approach for detection of Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks. In Grayhole and Blackhole attacks, the malicious nodes intentionally disrupt the packet transmission in the network by sending incorrect routing information. It is challenge to keep the communication route free from such attackers. In detection approach, an intermediate node receiving the abnormal routing information from its neighbor node which considers that neighbor node as a malicious node. An intermediate node continuously computes the PEAK value after an each time interval. An intermediate node received the RREP message and then analysis neighbouring node sequence number higher than the calculated PEAK value, if condition is true, marked as DO_NOT_CONSIDER; the node sending RREP is marked as malicious node in the routing table. Each intermediate node inserts the information about the malicious node in replay message. Each node upgrades the malicious node in routing table when it receiving replay packet [3]. Source node sending RREQ also appends a list of malicious nodes to inform other nodes in the network about the existence of attackers. An introduced approach only increases the PDR with negligible difference in routing overhead. It does not consider parameter improvements like end to end delay and network lifetime.

In [7] introduced a mechanism to detect the Gray Hole Attack. Grayhole attack degrades the overall system performance by using malicious activity. Modified AODV Protocol is used to detect the Gray Hole Attack. The proposed method computes the peak value and verifies whether the sequence number of packet is less than or not. The Routing table sequence number, Reply packet sequence number and Elapsed time of adhoc network are used to compute the peak value. Once the node detected, it cannot broadcast any alarm message. Each node maintains the data structure in their local RAM which known as black list. The FALSE REPLAY is the responds which are identified as malicious node such as black/gray hole [4]. Depending on the number of FALSE REPLY from the node it decides to be black listed or not. Using this approach, gray/malicious node is added to black list and eliminates normal nodes to enter in black list. However the false reply threshold value is static.

In [8] proposed a new Blackhole attack detection method. The packet loss can be occurred in numerous way such as link broken, transmission errors and various attacks caused by malicious nodes. To solve this packet drop problem, the proposed system introduced an AODV based detection mechanism. The AODV protocol uses two parameter types, one is sequence number and another one is hop count. The sequence number has fresh information about network and hop count describes shortest path information. In Blackhole attack, the malicious nodes are accepting the RREQ message from its neighbours and highly increase the sequence number of the destination. Finally send RREP message back to source [5]. The malicious node takes the advantage assigning big sequence number in a route reply message and able to redirect the route. An introduced detection mechanism efficiently achieves low End-to-End Delay and high Packet Delivery Ratio. However the efficient detection of malicious nodes is still investigated.

In [9] introduced a Novel Approach for Preventing Black-Hole Attack in MANETs. The clustering mechanism is introduced in Ad-hoc On-demand Distance Vector (AODV) routing protocol for detection and prevention of black-hole attack. If the source node is take place in one cluster and destination is the member node of another cluster then the packet transmission will takes place through there cluster heads. The source node sends the Query REQuest packets through the intermediate cluster head to destination. Then check points verifies whether the intermediate node forward the packets correctly or not. The check points (CP) keeps the details of number of packets received and transmitted by each node. The probability of packets received at destination is defined as the ratio of number of packets received by destination and the number of packets broadcasted by source node. If $P_d < T$ the check points starts the malicious node detection process. If $P_d > T$ then the source node receives the acknowledgement from the destination [6]. In this approach, the packet loss exceeding 20% of the total packets sent by the source node the CP

initiates the black hole detection mechanism. Finally the malicious nodes are suspended from its route. However an introduced mechanism only considered the packet delivery ratio.

In [10] introduced a Modified DSR protocol for detection and removal of selective black hole attack in MANET. In selective Blackhole, the malicious nodes drop the packets selectively. The detection of Grayhole attack is difficult than black hole attack. An intrusion detection system is introduced for detect the Grayhole attack. The IDS nodes are in licentious mode to detect the malicious activity in number of data packets being forwarded by a node. Source node sends the request message to destination. Then destination starts Grayhole detection process by sending QREQ which is used for finding the number of data packets forwarded by that node, to its next hop node. The neighbour sends back a QUERY REPLY (QREP) packet to the destination node D [7]. The replay packets contain the number of data packets a node forwarded to its next hop neighbor in the source route. This discovery process starts when data packet loss exceeds 20% of the total packets sent by the source node. The malicious node behaviours is analysed and detected through this method. However it achieved high computation cost.

In [11] introduced an intrusion detection and adaptive response mechanism in Manet. The mobile Adhoc network is vulnerable to variety of attacks such as Blackhole, Grayhole and etc. To solve this problem IDAR is introduced which utilizes a combination of both anomaly based and knowledge based intrusion detection mechanism [8], it protect the networks from various attacks. The IDAR operates in three main stages. There are network monitoring & data collection, training, and testing. The IDAR continuously monitors the network and dynamically collects data for intrusion detection and prevention throughout the network's lifetime. The training process describes the usual behaviour of the nodes in network. The testing phase consists of an intrusion detection, attack identification, intruder identification; and adaptive intrusion response. An anomaly based intrusion detection scheme identifies any intrusion such as black hole, Grayhole in the network. In attack identification phase, the rule based mechanism is used to identify the attacks. The manager node starts the intruder identification process when attack is once identified. However, it has routing overhead.

3. Comparison of methodologies

S.No	Title	Author name	Method used	Merits	Demerits
1	A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks	S. L. Dhende , Prof. Mrs. D. M. Bhalerao	Defence mechanism	It detects multiple black hole nodes with minimum delay and control overhead	The network performance improvement is still investigated
2	Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks	Rutvij H. Jhaveri , Sankita J. Patel and Devesh C. Jinwala	AODV based detection mechanism	It achieves highly safe and secure communication It increases the packet delivery ratio	It does not considered routing overhead and end to end delay improvements
3	A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks	Ashok M. Kanthe, Dina Simunic and Ramjee Prasad	Modified AODV method	High throughput Low packet drop rate High packet delivery ratio	The false reply threshold value is static
4	Blackhole Attack and Detection Method for AODV Routing Protocol in MANETs	Vipin KhandelwalM and Dinesh Goyal	Blackhole Attack and Detection Method	It isolates the malicious nodes	An efficient detection method will be needed.
5	A Novel Approach for Preventing Black-Hole Attack in MANETs	Rashmi and Ameeta Seehra	Cluster based Black-Hole Attack prevention approach	High detection rate High throughput	It only considered the packet delivery ratio for detection approach
6	Modified DSR protocol for detection and removal of selective black hole attack in MANET	M. Mohanapriya, Ilango Krishnamurthi	Intrusion detection system	Low packet loss Low energy loss	Huge computational cost
7	An intrusion detection & adaptive response mechanism for MANETs	Adnan Nadeem, Michael P. Howarth	An intrusion detection and adaptive response mechanism	High network performance It has high success and low false alarm rate	It has network overhead

The numerical proof of these of methodologies has been given and discussed in the detailed manner in the following sections.

4. Numerical results

This performance evaluation is conducted in terms of parameters called packet delivery ratio and end to end delay. The graphical illustration of these parameters in terms of various research methodologies is given and discussed detailed in the following sub sections. The various research methodologies that are analysed in this work are listed as follows

The various research methodologies that are analysed in this work are listed as follows

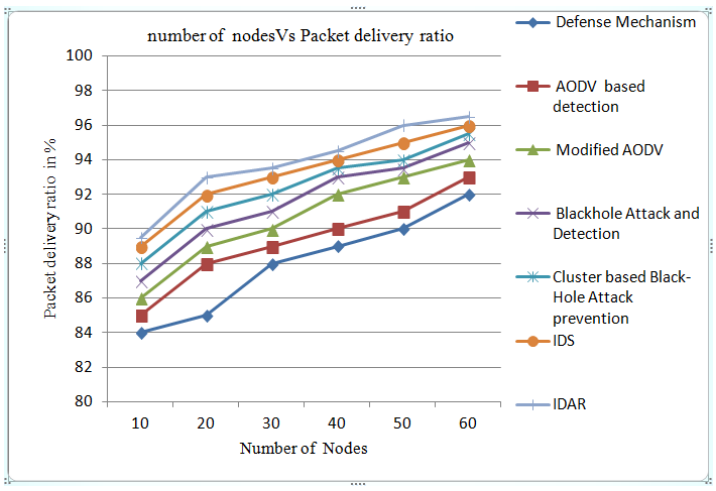
- Defense mechanism
- AODV based detection mechanism
- Modified AODV
- Blackhole Attack and Detection
- Cluster based Black-Hole Attack prevention
- Intrusion detection system (IDS)
- An intrusion detection and adaptive response (IDAR) mechanism

4.1. Packet delivery ratio

It is defined as the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$Packet\ delivery\ ratio = \frac{\sum Number\ of\ packet\ receive}{\sum Number\ of\ packet\ send}$$

Figure 1. Packet delivery ratio

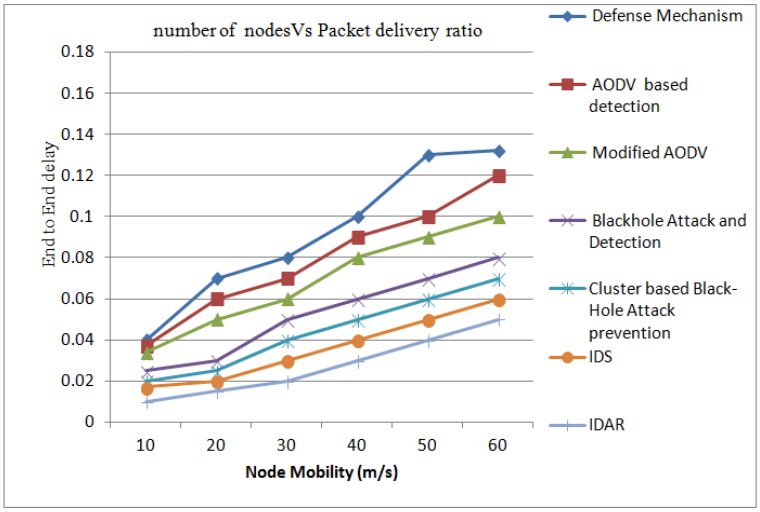


In figure 1, the comparison of literature methods in terms of Packet delivery ratio is given. In x-axis the number of nodes is taken whereas in the y-axis the Packet delivery ratio is taken. From this graph it can be proved that the intrusion detection and adaptive response mechanism has better Packet deliver ratio than the other techniques.

4.2. 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.

Figure 2. End To End delay



In figure 2, the comparison of literature methods in terms of End To End delay is given. In x-axis the Node mobility is taken whereas in the y-axis the End To End delay is taken. From this graph it can be proved that an intrusion detection and adaptive response mechanism has better End To End delay than the other techniques.

5. Conclusion

Black Hole Attack and Grayhole is a main security threat which affects the performance of the routing process in Manet. The attack detection is the main matter of concern. Over the recent past years, many researchers proposed their own method for packet drop detection to improve the packet transmission (Packet delivery ratio). In this paper, many advanced methodologies have been discussed and they are analyzed to find the most suitable and efficient method. The simulations are conducted and the results show that an intrusion detection and adaptive response (IDAR) mechanism is the better method than the other techniques in terms of packet delivery ratio and end to end delay.

5. References

1. Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami. EAACK-A Secure Intrusion-Detection System for MANETs. *IEEE transactions on industrial electronics*. 2013; 60(3).
2. C.V. Anchugam, K. Thangadurai, Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis. *Indian Journal of Science and Technology*. 2015; 8(13), 1-10.
3. Reza Amiri, Marjan Kuchaki Rafsanjani and Ehsan Khosravi. Black Hole Attacks Detection by Invalid IP Addresses in Mobile Ad Hoc Networks. *Indian Journal of Science and Technology*. 2014; 7(4), 401-408.
4. Y. Haripriya, K. V. Bindu Pavani , S. Lavanya, V. Madhu Viswanatham. A Framework for detecting Malicious Nodes in Mobile Adhoc Network. *Indian Journal of Science and Technology*. 2015; 2015; 8(S2), 151-155.
5. S. L. Dhende, Prof. Mrs. D. M. Bhalerao. A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks. *International Journal of Engineering Research & Technology (IJERT)*. 2012, 1(6), 490-495.
6. R.H. Jhaveri, S.J. Patel, D.C. Jinwala. A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks. *IEEE*, 2012; 556-560.
7. A.M. Kanthe, Dina Simunic, Ramjee Prasad. A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks. *International Journal of Computer Applications*. 2012; 53(16), 23-30.

8. V.M. Khandelwal, Dinesh Goyal. Blackhole Attack and Detection Method for AODV Routing Protocol in MANETs. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 2013; 2(4), 1555-1559.
9. Rashmi, Ameeta Seehra. A Novel Approach for Preventing Black-Hole Attack in MANETs. *International Journal of Ambient Systems and Applications (IJASA)*. 2014; 2(3), 1-9.
10. M. Mohanapriya, Ilango Krishnamurthi. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers and Electrical Engineering, *Elsevier*. 2014; 40(2), 530-538.
11. Adnan Nadeem, M.P.Howarth. An intrusion detection & adaptive response mechanism for MANETs. *Elsevier*. 2014; 13(Part B), 368-380.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

***Citation**:*

P.Rathiga. An Adaptive Identification and Prediction of Attacks in MANET: A Survey. *Indian Journal of Innovations and Developments.* 2015; 4 (6), October.