International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

Se-Eaodv to Detect and Prevent Black Hole Attack in Manets

Khushbu, R.K Bathla

Abstract: ***The security of the data which is transferred from source to destination is of prime importance in the mobile ad hoc network (MANET) or any kind of network to be very precise. If the data gets lost then the entire purpose of deploying and creating the network fails. Mobile ad hoc networks suffer from various attacks out of which black hole attack is considered the most dangerous one because in this attack the venomous node release all the packets received by it. The authors in EAODV has used the concept of fake route request packets to identify the black hole nodes in the grid. The proposed technique detects the malicious black hole node using the sequence numbers. The performance of the network has been examined based on end to end delay, packet delivery ratio, detection time, throughput and remaining energy. These parameters have shown improvement over the existing scheme.***

Keywords: MANETs, Black hole attack, Sequence number, EAODV, RREQ, PDR

I. INTRODUCTION

A MANET is a collection of wireless mobile devices that dynamically frame an arbitrary and temporary network. In this network grid, mobile devices are linked with each other without any wires and communicate over radio waves. These networks are completely decentalised, and might work at any area without any assistance of any predefine infrastructure [1]. A MANET having essential qualities, for example, open medium, dynamic topology, distributed cooperation, absence of centralized authority and multi-hop routing. Due to these standards, wireless mobile ad-hoc network are defenseless against different attacks. Hence, by availing the benefits of routing protocol attacker could perform different attacks. For the fundamental capability of the network, security is the biggest critical challenge in the MANET [2].

AODV routing protocol is most preferably used in MANET [3]. In AODV protocol when a node wants to communicate with another node it transmits RREQ (Route REQuest) packet with special identifier to all its neighbors [4]. Black hole is an attack that makes use of route request packets of AODV protocol. In this, the attacker promote itself through the fresh path to the destination node even though the route is long. Black hole is divided into two types [5]: single black hole attack and collaborative black hole attack. This paper demonstrates the existing techniques that focuses on detection and prevention of black hole.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
Khushbu*, Research Scholar, Professor, P.hd Madhav University
Dr. R.K Bathla, Research Scholar, Professor, P.hd Madhav University

Section III explains the proposed technique and the experimental results have been described in Section IV. Conclusion to this paper has been discussed in the last section.

II. LITERATURE REVIEW

A routing algorithm is proposed in [6] based on sending found packets so as to amplify the accuracy of detecting and removing malicious nodes. According to the approach suggested, malicious nodes in the network are identified by routing packets including the address of the impossible destination knot via forged route request (RREQ) and route reaction (RREP). They are then removed by sending a RREP message from routing node tables. This paper has been designed to improve network traffic, detect short, secure routes, detect several malicious nodes and optimize packet delivery, performance, and overhead criteria. The results of the simulations showed that the percentage of data packets delivered by the proposed algorithm was higher than those of the IDS algorithm. In addition, the delay of the proposed method was lower than other methods thanks to the accuracy of black hole detection, the lack of a number of RREQ and RREP conditions and the rapid routing detection process. The above variables have contributed to a performance optimization. The authors in [7] propose to increase the likelihood for Black hole nodes to be found and prevented in MANETs an improved confidence detection algorithm. The proposed system measures the conduct of each node using different confidence metrics, including the relationship between the sensor nodes, the confidence in the social and service attributes, and metric trust QoS. Sensor node behavior is defined by each node's contact and mobility behaviour. When the routing is done using the Zone Routing Protocol (ZRP), the process avoids black-hole nodes in MANET. The privacy of the data is therefore retained by the method proposed. In terms of different combinations with and without confidence, the proposed approach is checked. The result shows that the proposed method is effective through various QoS metrics like overall throughput, packet loss, energy consumption, trust level, false acceptance rate and missed detection rate. A updated and improved RID-AODV protocol based on the preceding mechanism: RID-AODV is proposed in paper [8]. The change proposed is focused on the development of dynamic blacklists for each network node. According to criteria, every node depends on the number of mismatches of the hash values of the packets it receives compared to certain threshold values, and it may decide to add or delete the other nodes from or to the blacklist by adjusting the roundtrip time (RTT).

The threshold is a mobility feature to annul the impact of a standard connection failure. In this paper [9] a proposed optimized fuzzy-based intrusion detection system is presented as an automation of the development of a fuzzy system using the Adaptive Neuro-Fuzzy Inference Method (ANFIS) for initializing the FIS. The authors have suggested in this research [10] that Black hole attacks in the ad hoc mobile networks (MANET) be observed and prevented. The cuckoo search algorithm is used by the use of the classifier known as artificial neural network (ANN), for the optimisation of node properties by Objective Functions. By using ANN, the route is known as a black hole attack. Then parameters of performance such as performance, delay, energy consumption and bit error rate are determined.

This paper [11] offers a new approach based on building a reputation system which helps AODV protocol to choose the best path to its destination if more than one route is possible. The proposed protocol enhances the usage by gathering observations of the watchdogs in AODV and disperse them through a low overhead approach to all nodes within the network. Therefore, as a black hole travels continuously, the proposed protocol takes account of the detection problem. The hybrid and clustering security mechanism against several nodes of the dark hole is discussed in paper [12]. The scan results show that the strategy proposed is able to identify and efficiently isolate the malicious nodes in the network. This would improve the capacity of the network to broaden the performance, reduce the network failure and delay. The NS-2.33 will be used as part of the simulator instrument. A clustering method was suggested in the MANET's AODV routing protocol to detect and prevent black-hole attack[13]. Per cluster member pins once to the cluster head and senses the distinctive difference between the amount of data packets that the node receives and sends. All the nodes hide the malicious nodes from the network when anomalies are detected. The system performance analysis was carried out using ns2 simulator for Packet Delivery Ratio (PDelr) and Detection Rate (DR).

III. PROPOSED TECHNIQUE

The technique proposed aims at detecting the black hole attack on the basis of the source node sequence number. The RREQ packet is sent to find the way to the original target in the source node. All nodes retransmit the route request until the destination node is reached. The route request will be send route replies to the source node if the destination node is received. At the source node, the maximum sequence number can be identical to the sequence number at the destination node in addition with the hop count. Because at each hop, the sequence number is incremented by 1.

$$Max\ SQ = Sq_{dst} + h$$

Where h is the hop count, Sq_{dst} is the sequence number at the destination node. Hence, the source node will compute maximum sequence number possible for each path. If for any path, the sequence number is greater than desired sequence number then the path will be suspected for the black hole node. To perceive black hole node in that particular path, the source node would now send fake RREQ packets. These packets will be unicasted over single suspected path. If there will be black hole node on this route, the node will send RREP. The originator of the RREP node will be detected as the black hole node. The source node will inform the node in this suspected path about the malicious node so that nodes do not send any packet to malicious node. The source node will send data to the destination over the shortest path that do not contain any black hole node.

Pseudo Code:

BEGIN

1. Suppose N is the number of nodes. Nei_j is the neighbor set of the $Node_j$

2. for i=1:N

2.1 for j=1:Nei

2.2 Node(i) broadcasts RREQ packet to Nei(j)

2.3 If Nei(j)==Destination node

2.4. Route Reply()

2.5 Else

2.6 Goto step 2.2

2.7 End if

2.8 End for

2.9 End for

Route Reply()

3. Destination node formulates all paths to source node

4. Send route reply to source node

5. Compute maximum sequence number

6. Compare sequence number received with desired sequence number possible

7. If received seq no > Desired Seq no

7.1 Send fake RREQ packet over the path

7.2 If RREP received

7.3 Mark originator of RREP packet as malicious

7.4 Else

7.5 Node is genuine

7.6 End if

7.7 Else

7.8 Path is devoid of any malicious node

7.9 End if

8. Choose shortest path from malicious node-free paths to forward data to destination node

IV. RESULTS

This study showcases the black hole detection technique based on sequence number analysis. This is a modification to the existing technique which uses the fake route request packets to notice the malicious black hole nodes from the network. Both the schemes have been implemented in the network simulator 2.35. The simulation parameters used are:

Parameter	Value
Number of nodes	50
Traffic type	CBR
Payload	512 bytes
Queue Size	50
Network area	1000*1000 m^2
Routing protocol	AODV
Mobility model	Random way point
Initial Energy	50 Joules
Propagation	Two Ray Ground

Table 4.1 Simulation Parameters

The graph 4.1 below shows the remaining energy for both the schemes. Initially all the nodes in the network were supplied with energy of 50 Joules. At the end of the simulation, the network was left with energy of 35.87 Joules with the proposed scheme and 31.28 Joules with the existing scheme.

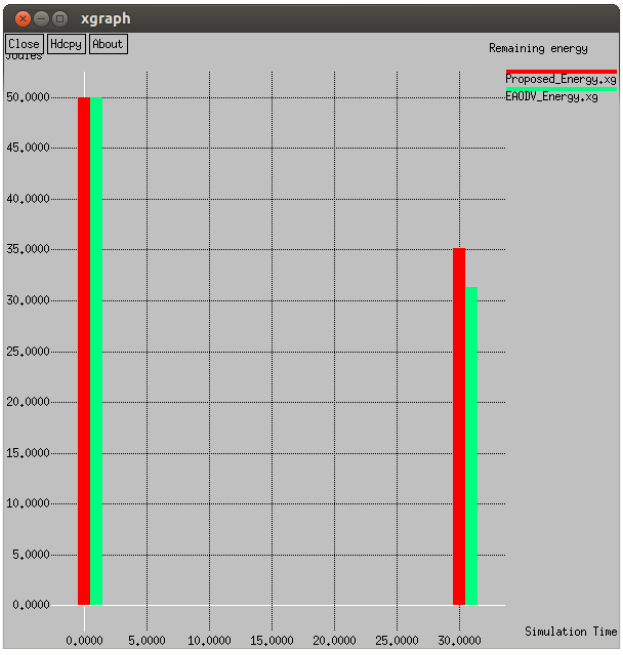

Figure 4.1: Remaining Energy comparison

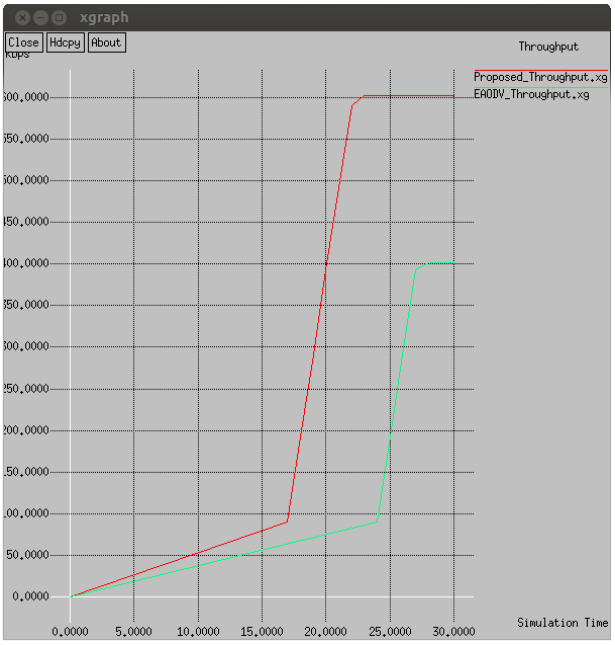

Figure 4.2: Throughput comparison

This graph 4.2 shows the throughput achieved for both the schemes. The value of throughput for the existing scheme was 401 Kbps and for the proposed scheme was 602 Kbps. This indicates the destination node receives more data with the proposed scheme.

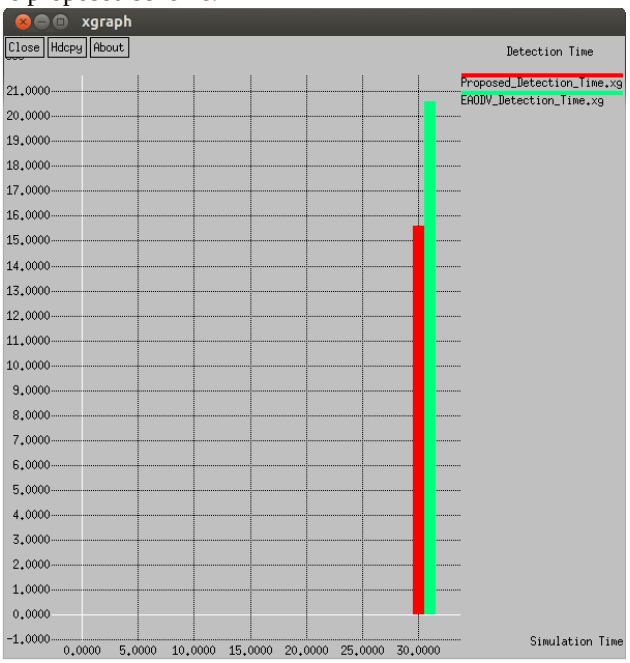

Figure 4.3: Detection Time comparison

This figure 4.3 shows the value of detection time for both the scheme. The proposed scheme took 15.6 seconds to detect the black hole nodes while the existing scheme took 20.6 seconds to detect the black hole nodes in the network matrix. The figure 4.4 depicts the value of packet delivery ratio obtained for both the schemes. The proposed scheme has higher PDR of 0.98 than existing time which achieved PDR of 0.97.

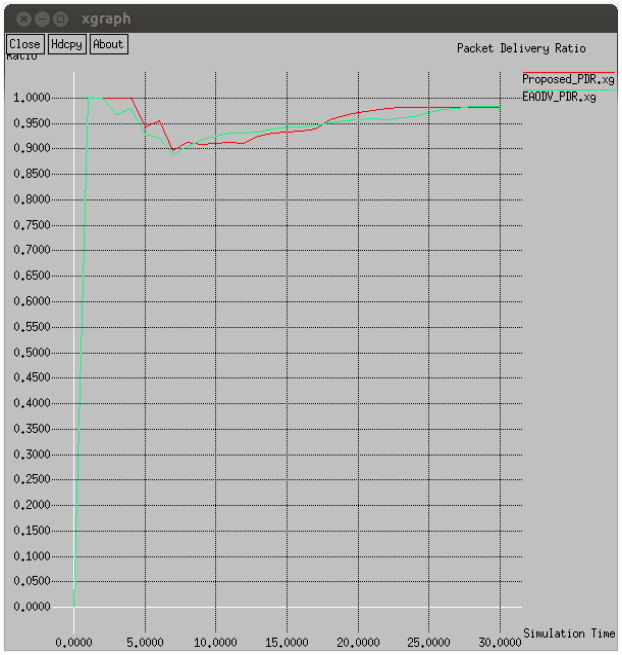

Figure 4.4: PDR comparison

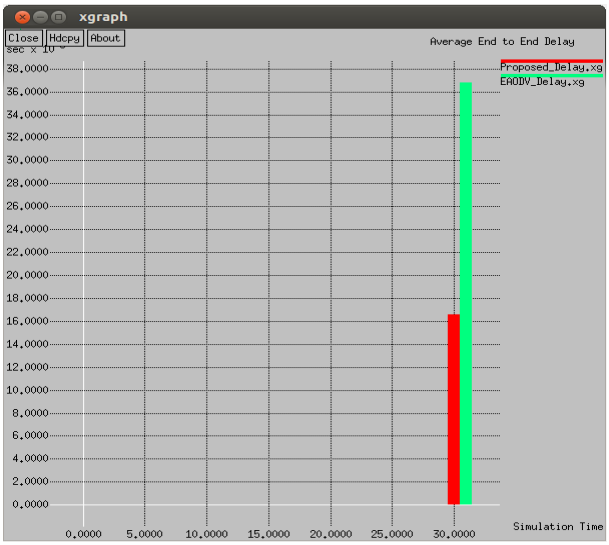

Figure 4.5: E2E Delay comparison

This figure 4.5 shows the value of end to end delay obtained for both the schemes. The proposed scheme has lesser end to end delay of 0.016 seconds while existing scheme has delay of 0.036 seconds.

Parameter\Scheme	Existing	Proposed
Detection Time	20.6 seconds	15.6 seconds
Remaining Energy	31.28 Joules	35.87 Joules
Throughput	401 Kbps	602 Kbps
PDR	0.97	0.98

Table 4.1: Results Comparison

V. CONCLUSION

This study focuses on black hole attack in mobile ad hoc networks. In this proposed work, the detection of black hole nodes was done by checking the expected value of sequence number of route reply packets that is received at the source node. The performance of both the schemes was compared based on end to end delay, packet delivery ratio, detection time, throughput and energy remaining in the network. The detection time, end to end delay for existing scheme as well as energy consumption of the network was more because the broadcasting happens twice, one for the fake route request packets and then for the real route request packets. Since the detection happens earlier in the proposed scheme since request packets are broadcasted just once, so the network also consumes lesser energy and experiences lesser delay. This allows the nodes to address more data to the destination node. This increases the throughput of the network as well. This helps us to conclude that the proposed scheme outperforms the existing scheme in the network.

The mobile ad hoc networks also suffer from attacks such as wormhole attack or sink hole attack etc. In future, the work can also be done to make network secure from such attacks.

REFERENCES

1. Aarti, Dr SS. Tyagi, “Study Of Manet: Characteristics, challenges, application and security attacks”, International Journal of Advanced Research in Computer Science and Software Engineering 3.5, vol. 3, no. 5, pp. 252-257, May-2013.
2. Shendurkar, Ms Ankita M., and Nitin R. Chopde. "A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET." International Journal of Engineering Trends and Technology (IJETT), vol. 9, no. 8, pp. 394-399, March-2014.
3. Sandeep Lalasaheb Dhende, S. D. Shirbahadurkar, S. S. Musale, Shridhar K. Galande, “A survey on black hole attack in mobile ad hoc networks”, 2018 4th International Conference on Recent Advances in Information Technology (RAIT).
4. Avni Tripathi, Amar Kumar Mohapatra, “Mitigation of Blackhole attack in MANET”, 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN).
5. Khemariya, Neelam, Ajay Khunteta, and Krishna Kumar Joshi. "A Robust Technique for Secure Routing against Blackhole attack in AODV Protocol for MANETs." International Journal of Scientific & Engineering Research, vol. 4, no. 6, pp. 1179-1189, June-2013.
6. Taher Delkesh, Mohammad Ali Jabraeil Jamali, “EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs”, Journal of Ambient Intelligence and Humanized Computing, March 2018.
7. J. Manoranjini, A. Chandrasekar & S. Jothi, “Improved QoS and avoidance of black hole attacks in MANET using trust detection framework”, Computational Intelligence and Capsule Networks, Jun 2019.
8. Rushdi A. Hamamreh, “Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks”, Recent Advances in Cryptography and Network Security, October 31st 2018.
9. Mohamed Abd-El-Azim, Hossam EL-Din Salah, and Menas Ebrahim, “IDS against Black-Hole Attack for MANET”, International Journal of Network Security, Vol.20, No.3, PP.585-592, May 2018.
10. Meenanshu Gupta, Varun Jasuja, “Improvisation of QOS Parameters by Detecting and Preventing the Black Hole Attacks using Artificial Intelligence Techniques”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 6 Issue II, February 2018.
11. Qussai M. Yaseen, Monther Aldwairi, “An Enhanced AODV Protocol for Avoiding Black Holes in MANET”, Procedia Computer Science, Volume 134, 2018, Pages 371-376.

12. Veerpal Kaur, Simpel Rani, "A Hybrid and Secure Clustering Technique for Isolation of Black hole Attack in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 3, March 2018.
13. Rashmi, Ameeta Seehra, "Detection and Prevention of Black-Hole Attack in MANETS", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Jul-Aug 2014.