Selfish Node Detection and Prevention Based on SDSR in Infrastructure-Less Networks

Anusha Chintam (anusha.rohini07@gmail.com)
Vignan's Institute of Information Technology https://orcid.org/0000-0002-7169-632X
A. Sravani
Vignan's Institute of Information Technology
T.V. Madhusudhan Rao
Vignan's Institute of Information Technology

Research Article

Keywords: wireless mesh network, black hole, gray hole, NS2, SDSR, decentralization, selfish DSR

Posted Date: June 2nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-455766/v1

Abstract

Wireless mesh network formed temporarily by using mobile hosts (nodes) without the help of any centralized and cooperate to dispatch the data packets through wireless links over the network. Due to this decentralization, each node act as both router as well as host for dispatching packets in the network. Because of a dynamic nature that is the mobility nature of the node in a network is vulnerable to various types of attacks. Some of the attacks are gray and black hole attacks. These attacks are advertised incorrect information regarding the shortest path to the sink node. This paper proposes a secure Dynamic Source Routing (SDSR) for providing a secure and safe route between the origin and sink nodes which identify and remove the gray and black hole nodes in the network. The proposed work is simulated by using the NS2 simulator tool and got the better performance for considered performance variables such as packet delivery ratio, throughput and node overhead. The simulation results give better performance compared to normal DSR and selfish DSR with increased packet delivery ratio and throughput and with decreased overhead of the network.

Introduction

MANET is a group of mobile hosts to form a network temporarily with wireless interface and without use, any aid of any fixed infrastructure .the presence of decentralization each node in a network act as both router as well as host for forwarding the data from one node to another node. Therefore the wireless mess networks face many security vulnerable attacks such as denial of service attack, imprecation, active route interfering. Gray hole and Block hole attack are one of the attacks in wireless networks [1, 2]. These attacks send the false route replay information to the sink node to find the route finding process. The Gray hole attack might take place because of the malicious nodes that are consciously misbehaving and has smashed the node interface. A black hole attack is an intentional malicious activity that sometimes drops all or some packets are dropped while forwarding to the destined node[3].to detect or remove these selfish nodes from the network assign the Armstrong number to each node as a node id in case of DSR routing.

1.1.DSR Routing Protocol:

DSR (Dynamic Source Routing) is an on-demand routing protocol of wireless networks. In DSR, the connection between the two nodes is established only when it is required [4, 5]. It contains two messages for communication they are route request and route replay.

Route Request Message (RREQ): For finding the path to reach the sink, the origin node start by broadcasting the RREQ message to all its neighbors [6]. The RREQ consists of the source address, a route confirmation field, destination host address and a unique identification number as shown in fig.1.

Rout Reply message (RREP)

In a network every node observing the hop status to its neighbour's nodes during the route finding. Once the route is found in the target node, dispatch the RREP message to notify the other nodes in the hop list shown in fig. 2.

1.2.Black hole attack:

A black hole attack is a type of denial of service attack. In which the selfish node unicasts the incorrect RREP message to the origin node with the high sequence number for misguiding the source host might trust that is the ultimate destination for better performance of a network [7, 8]. Origin node S wants to send the data to the sink node D As shown in fig .3.here the node S broadcast the RREQ packet to all its neighbours. Now all the neighbour nodes after receiving the RREQ packet first check its routing table entries. If they found the shortest path to the sink node then they send the RREP message to the origin node. However, here the selfish node without checking any routing table entries for saving the battery to dispatch its RREP message to the origin node S with B is a sink node. After received the selfish node RREP message source node start to send the data malicious node M then the malicious node continuously dropping the data packets and interrupts the control messages that may lead to the critical security issue in the network.

- **Gray Hole Attack**

The Gray hole attack might take place because of the malicious nodes that are consciously misbehaving and has smashed the node interface. During the route finding process first, the malicious node act as a trusted node and then may change to the selfish node vice versa [8]. This selfish node may drop some or all packets. The identification of this attack is difficult to compare a black hole attack why because of the ability of the state to change nature. As shown in fig .4, the node 4 act as a selfish node and send the incorrect message to origin node during route finding process and it drops all the packets coming from a specific node to all nodes.

Methodology

A methodology is used to identify and prevention of the black hole and gray hole attacks in the DSR routing protocol. In this method, for the identification of the selfish nodes, the source node takes the neighbour nodes opinions. The behaviour of a node in the mesh network shows its authentication [9]. The nodes should show their honesty for participation in the data communication process. For this product of an Armstrong number scheme is applied for the removal of black and gray hole attack in wireless networks. For the node, the identification process assigned an Armstrong number to each node as a node sequence number in the network. Which does not change. The origin node receives the RREP message from all its neighbour nodes. After receiving the RREP packet, the origin node verifies the product of the node sequence ID's in the neighbour count list to reach the sink node [10, 11]. The origin node also takes the opinion of the neighbour's about the replied node. Considered the wireless mesh network scenario shown in fig.6. Let the origin and sink nodes are H and G. The whole process is given by in different modules and shown in fig.5.

RREQ:

After assigning the Armstrong, number to each node in the network the origin H broadcast the RREQ message to all its neighbours during the route finding process. The neighbour node received the RREQ message and to the identification of its honesty send the RREP message to the origin node. The RREP packet consists of the neighbour node list [12] .this process continues until the RREQ message reaches the sink node G.

RREP:

All the nodes in a network hold their neighbour's list by using two tables. They are the decision table and neighbour count table. The neighbour count table holds the particular node and its neighbour's sequence number IDs and periodically updated the table. Another one is a decision table, which is useful for identifying the gray and black hole selfish node M shown in table 1.if origin node H want to send a message to the sink node G then it broadcasts RREQ to its neighbours [13]. The neighbour node fresh path to the sink node dispatches the RREP message to the origin. After receiving the RREP message, the source host broadcast its decision message to all its neighbours for taking the opinion about the replied node.

Neighbour's Node:

After receiving the decision message from the origin node the neighbour nodes give the acknowledgement with N packet means no packet through the replied node and Y packet means yes packet through some other path to the origin host. The origin node H waits for some time t for getting the decision packets from its entire neighbour's list [14, 15]. If the source H receives, the y packet then set the opinion as Y and if the origin node receives as N packet that updates its routing table with sequence ID of neighbours and set opinion as N [16, 17]. If the second table all opinion entries are, Y then the origin node conforms to the replied node as a black hole selfish node shown in table 2. In addition, if the second table all opinion entries are a combination of Y and N then the origin node conforms the replied node as gray hole selfish node shown in table 3.

Table 1: neighbour node count table for a particular node

Particular node	Neighbors
M	A,F,N

Table 2: decision table for black hole selfish node

Neighbours	Opinion of neighbours
A	Y
F	Y
N	Y

Table 3: decision table for gray hole selfish node

Neighbours	Opinion of neighbours
A	N
F	Y
N	Y

Simulation Results And Discussions

The proposed work is simulated by using the NS2 simulator tool to the DSR protocol. Constant bit rate (CBR) Traffic type, two-way ground propagation in a rectangle field of 1000m x 1000m with 80 nodes, IEEE Link layer MAC protocol, DSDV routing protocol parameters used by the simulator for simulation. An output trace file is a resultant of the simulation used to visualize, processing data with the help of a network animator (NAM) program, and got better performance for considered performance parameters such as throughput, node overhead and packet delivery ratio. The results of the simulation give the better performance compared to the SDSR, normal DSR and selfish DSR with increased throughput and packet delivery ratio. The overhead is decreased.

The following graph of nodes vs packet delivery ratio is shown in fig.7. For all considered protocols. The PDR is increased for SDSR and for normal DSR the PDR is zero in starting after the PDR value is increased and stopped to increase. For selfish DSR the PDR is constant in starting after some time the value of PDR is slightly increased and finally decreased due to state change nature of malicious node.

The graph of nodes versus overhead is shown in the following fig.8. The overhead of the SDSR protocol is zero because of the collecting of neighbour's opinions. The Overhead of the normal DSR is a little bit more compared to the selfish DSR because of the dropping of the packets.

The graph of nodes versus throughput is shown in the following fig.9. Initially, the throughput is decreased for all considered protocols and the number of node velocities is varied. After some time the throughput of the SDSR is improved, compared to remain normal and selfish DSR protocols.

Conclusion

The wireless mesh networks are unprotected from the malicious attacks .this paper explains some of the malicious attacks black and gray hole attack .and their detection and removal by using secure DSR.to make a normal DSR into a secure DSR assigned Armstrong product number scheme. For the node, the identification process assigned An Armstrong number to each node as a node sequence number in the network. Which does not change. The origin node receives the route replay message from its neighbour nodes. After receiving the route replay packet the origin node verifies the product of the node sequence ID's in the neighbor count list to reach the sink node. The origin node also takes the opinion of the neighbour's about the replied node. The simulation results give better performance compared to normal DSR and selfish DSR with increased throughput and packet delivery ratio. The overhead is decreased. In feature scope, the same methodology will be applied to the other classes of the wireless mobile networks protocols and compare with the proposed protocol secure DSR with the different network performance metrics.

Declarations

Funding: Not Applicable

Conflicts of interest: no potential conflict of interest in relation to the study in this Paper.

Availability of data and material: Not Applicable

Code availability: custom code.

Authors' contributions:

CH. participated in the design, performed experiments and analysis and wrote he paper; A and TV participated in the revisions of it.

References

1. Anuj Rana, Vijay Rana, and Sandeep Gupta, "EMAODV: technique to prevent collaborative attacks in MANETs," Procedia Computer Science, vol. 70, pp. 137–145,2015.
2. Mohan V. Pawar and J. Anuradha, "Network security and types of attacks in network,"Procedia Computer Science, vol. 48, pp. 503–506, 2015.
3. SapnaGambhir and Saurabh Sharma, "PPN: Prime product number based malicious node detection scheme for MANETs," in 3rd International Advance Computing Conference (IACC), IEEE, 2013.
4. Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile ad hoc networks," in ACMSE'04, April 2–3, 2004, pp. 96–97.
5. Ankita M. Shendurkar 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, pp. 394–399.

6. Vimal Kumar and Rakesh Kumar, “An adaptive approach for detection of blackhole attack in mobile ad hoc network,” Procedia Computer Science, vol. 48, 2015, pp. 472– 479.
7. Anusha, K. Chinnaiah,”An Efficient "An Efficient Secure Routing in Mobile Ad- hoc Networks Using HMAC", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 10, page no.359-367, October-2018.
8. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, “Prevention of cooperative black hole attack in wireless ad hoc networks,” in IEEE Proc. of Int’l Conf. on Wireless Networks, 2003.
9. Dokurer, Y. M. Erten, and C. E. Acar, “Performance analysis of adhoc networks under black hole attacks,” in IEEE Proceedings Southeast Con., 22–25 Mar. 2007, pp.148–153.
10. S. Bindra, A. Kapoor, A. Narang, and A. Agrawal, “Detection and removal of co-operative blackhole and grayhole attacks in MANETs,” in IEEE Conference on System Engineering and Technology (ICSET), 11–12 Sep. 2012, pp. 1–5.
11. Arvind Dhaka, AmitaNandal, and Raghuveer S. Dhaka, “Gray and black hole attack identification using control packets in MANETs,” Procedia Computer Science, vol. 54,pp. 83–91, 2015.
12. Nidhi Choudhary ; Lokesh Tharani, “Preventing Black Hole Attack in AODV using timer-based detection mechanism”, International Conference on Signal Processing and Communication Engineering Systems, Electronic ISBN: 978-1-4799-6109-2, IEEE, 2015.
13. Lu, L. Li, K. Y. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security, Vol. 2, pp. 421-425, 2009.
14. Pooja ; R. K. Chauhan, “An assessment based approach to detect black hole attack in MANET”, International Conference on Computing, Communication & Automation, Electronic ISBN: 978-1-4799-8890-7, IEEE, 2015.
15. Raza, M. U. Aftab, M. Q. Akbar, O. Ashraf and M. Irfan, “Mobile Ad-Hoc Networks Applications and Its Challenges”, Communication and Networks, Vol 8, No. 3, pp. 131, 2016.
16. Dorri, S. R. Kamel and E. Kheyrkhah, “Security Challenges in Mobile Ad Hoc Networks: A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol. 6, No.1, pp. 15-29, February 2015.
17. Nidhi Choudhary ; Lokesh Tharani, “Preventing Black Hole Attack in AODV using timer-based detection mechanism”, International Conference on Signal Processing and Communication Engineering Systems, Electronic ISBN: 978-1-4799-6109-2, IEEE, 2015.
18. Lu, L. Li, K. Y. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security, Vol. 2, pp. 421-425, 2009.

Figures

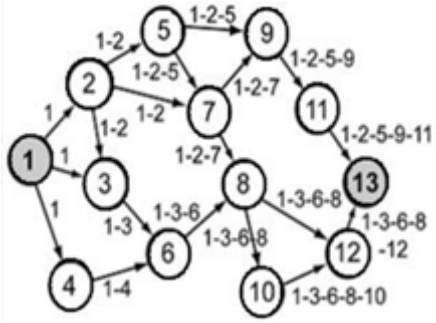

Figure 1

Route Discovery in DSR

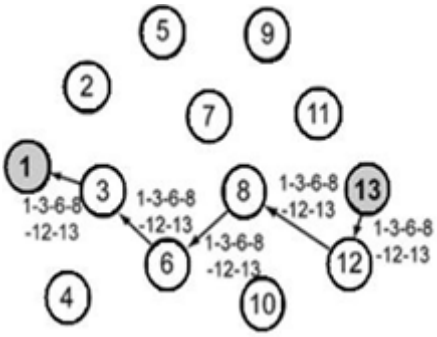

Figure 2

Route Reply in DSR

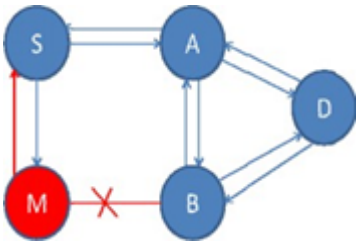

Figure 3

Black Hole Attack

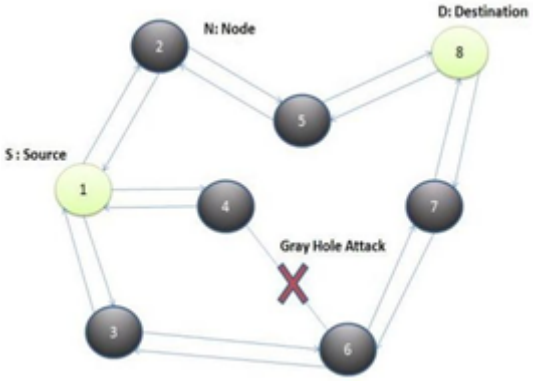

Figure 4

Gray Hole Attack

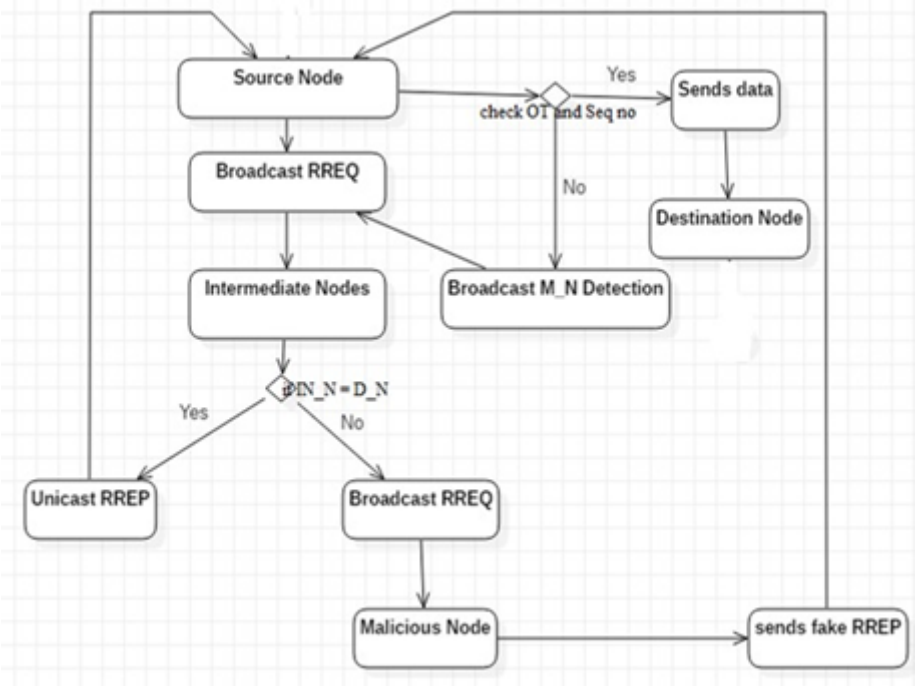

Figure 5

Proposed system architecture

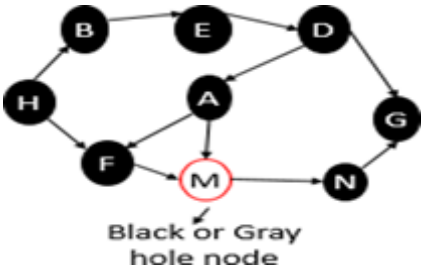

Figure 6

Network Scenario

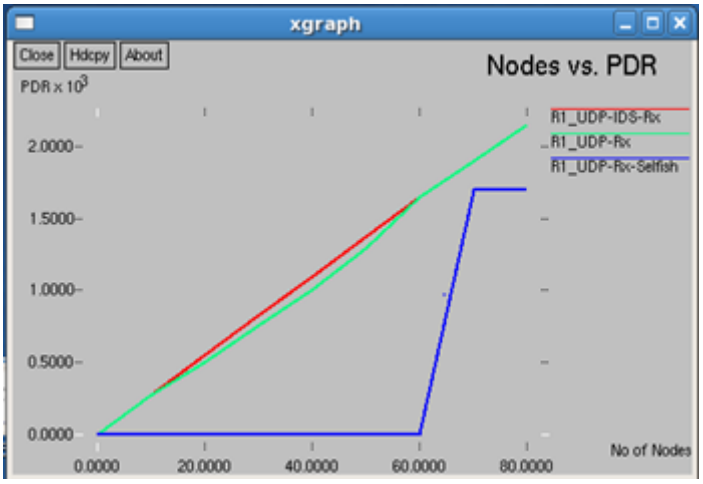

Figure 7

Nodes vs. PDR

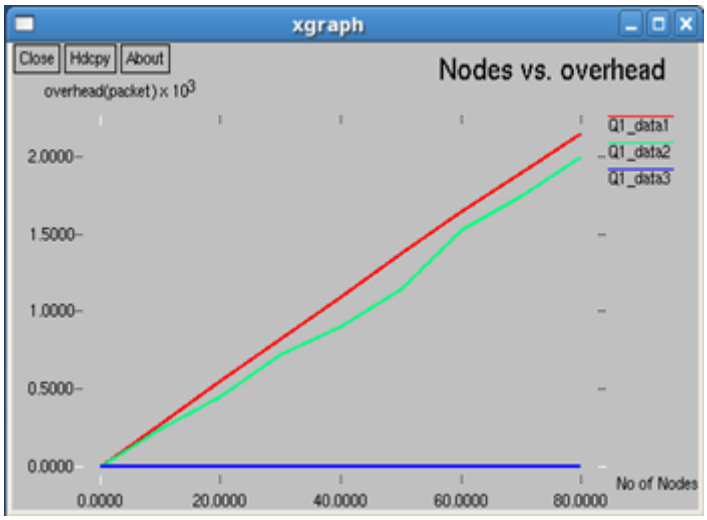

Figure 8

Nodes vs. Overhead

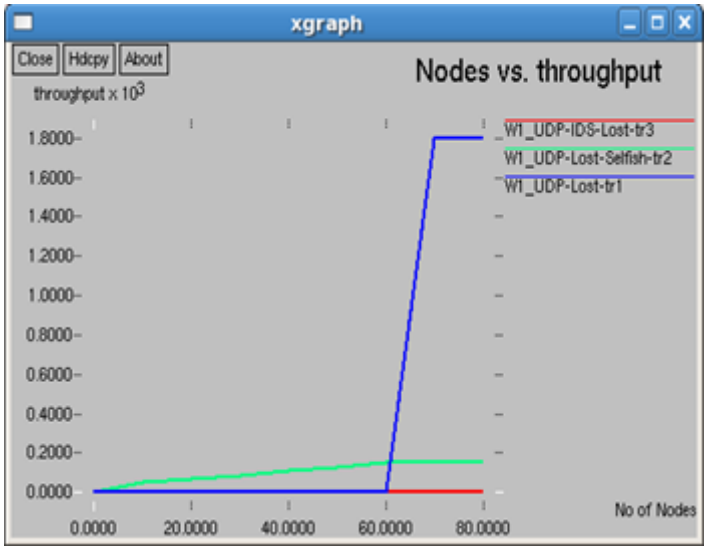

Figure 9

Nodes vs. Throughput