# Classifier based scheme to detect and avoid black holes in DSR based MANET

T.Roja [1], B.Anandakumar [2]
[1]M.Phil. Scholar, [2]Assistant Professor
[1]Department of Computer Science,
[1]Rathinam College of Arts and Science, Coimbatore, India

**Abstract: Wireless mobile ad hoc networks are dynamically changed and self-configuring network with freely movable nodes. Communication range between the mobile nodes in ad-hoc network is limited; hence several hopes are needed in a network to transmit a packet from one node to another node. In mobile ad hoc network, some nodes may inconsiderately decide only to cooperate partially and update false information regarding its active nodes. This behaviour of black holes could then degrade the overall data accessibility which results into performance degradation of overall network. However, the proposed scheme detects the black holes by modifying the original DSR routing algorithm. This research work, proposed a classifier based scheme for detecting and avoiding the black holes and perform the simulation using Network Simulator 2.34.**

**Keywords: Mobile Ad hoc Networks, DSR, Self-configuring, Cost-intensive, Black hole**

## I. Introduction

Ad hoc network refers to a network connection built for a single session and does not require a wireless base station and a router, it is a temporary network association made for some particular reason like for sending date from one device to other. If the network is set up for a long period of time, then it is just a plain old local area network.

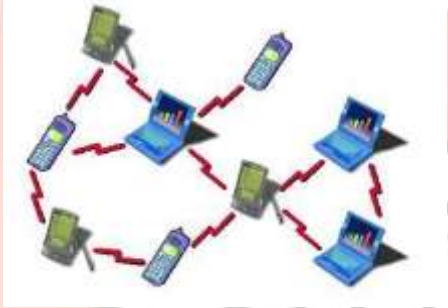

Figure 1.1: Ad hoc Network

It is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. Adhoc networks consist of routable network properties where each node act as a "router" to forward the traffic to other targeted node in the network.

The Dynamic Source Routing protocol is used in the multi-hop wireless ad hoc networks of mobile nodes without any existing network infrastructure and it configure the route by itself. The advantage of DSR is routing information maintenance is not required for the intermediate nodes in order to route the packets they forward. The DSR protocol has two key mechanisms, that is Route Discovery and Route Maintenance.

**Example :** The route discovery procedure is shown in the following figures with start node S1 and destination node S7.

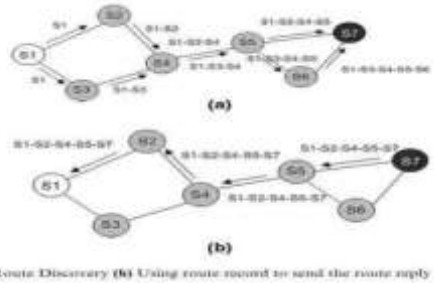


Figure:-1.2 Example for DSR

The destination node S7 gets the request through two paths such as from node S5 and node S6. It chooses any one path from the available two paths based on the route records in the incoming packet and reverse path to send the route reply to the source node S1. This example shown the route record status ate each hop to reach the destination from the source node. Here, the selected route between the source node S1 to destination node S7 through S2,S4 and S5.

**Attacks in MANET**

Wormhole Attack Malicious nodes create a wormhole. It is a link of less delay from one part of a network to another portion of the network in which the malicious node forwards the packets to the other malicious node. It is a network layer attack. In this type of attack, message is captured from the one region of network and replaying in other region. The attacker gather all message and other retransmits to make destination unreachable from network. Black hole Attack Attacker node broadcasts good paths to the node falsely during the route-establishment process in the case of reactive routing protocols, or in the form of route update messages in proactive routing protocols. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them. This make destination system unreachable in network like the denial of service attack. Sybil Attack is effective on routing protocols, accumulation of the data, unbiased resource allocation and misbehaviour detection. Sinkhole Attack A malicious node forges the routing information of the incriminated node and makes that node more attractive to the adjacent nodes. The adjacent nodes choose the incriminated nodes as their next-hop to route the data. Cloning Attack A rival node uses the identity of a compromised node and it secretly introduces the copies of the compromised node. These nodes can commence an attack that will be the downfall of the sensor network.

In a Black hole attack, a node which is called malicious node will absorb all the network traffic towards them and discard all the packet. If we want to catch the black hole attack, when malicious node checking its routing table it directly send a fake RREP with largest sequence number and smallest hop count to prove that it has the minimum path to reach the destination. By this way we can catch the black hole node in the network. Source node gets the more than one RREP from the different node but it is choose the RREP from the malicious node because that has a largest sequence number. The source node ignores the RREP which are not coming from the malicious node and then malicious node drops all the packets rather better to forward further to the destination node.

The malicious node takes allthe route towards them and attack all the RREQ packet. Malicious node generates the fake RREP and that will be delivered to the source node that it does know the path for destination. By this way source node assumes that it is the next node to reach the destination so it will send the packet to the malicious node and malicious node will be remove all the packets which are comes from the source node.

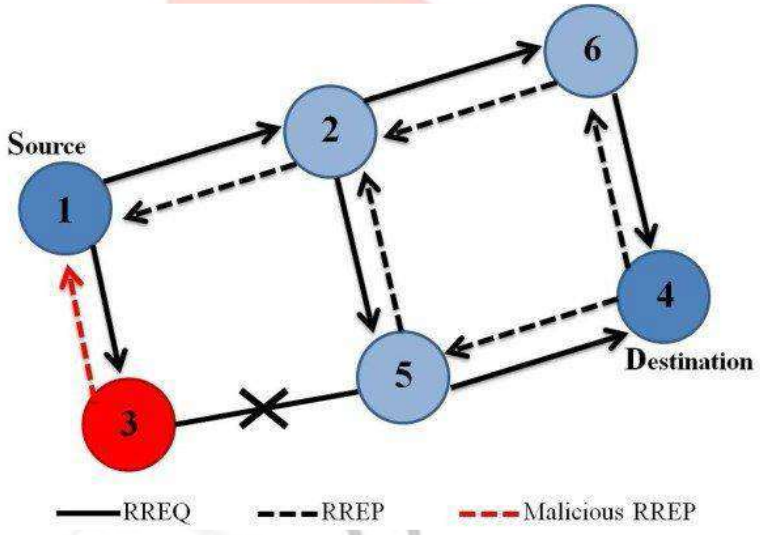


Figure:-1.3 Black Hole attack

Single black hole attack and Collaborative black hole attack are two types for the black hole attack. In the network if all the network traffic is switched to single node, it is called single black hole attack which is malicious node and it will drops all the packets. In collaborative black hole attack, there are many malicious nodes which are work together to switch normal routing information towards the malicious node and assemble that route according to them. Some researchers had work on black hole attack and provide methods to detect malicious nodes but that is not sufficient to solve the black hole problem and the more detection method should be initiated to solve the black hole attack.

## II. RELATED WORK

Rajesh Sharma et al. They had discussed a solution on the basis of reputation method to solve routing issues raised by misbehaving nodes [1].

Santhosh Krishna B. Vet et al. The author focus on single and multiple black hole attacks. The implementations of black hole comprises active routing misbehaviour and forwarding misbehaviour & design and build our prototype over DSR and test it in Network simulator 2 in the presence of variable active black hole attacks in highly mobile and sparse networks [5].

Isaac Woungang et al. deliver a innovative structure for Detecting Black hole Attacks in MANETs is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake route request packets to catch the malicious nodes [6].

Poonam K Gar et al. They had discussed and proposed a new algorithm to find route to the destination as a weighted average of the trust value of the nodes in the route, with respect to its behaviour observed by its neighbouring nodes and the number of nodes in the route is calculated [9].

Sangheetaa Sukumran et al. proposed a solution to tries to identify a route, its route request will be forwarded by the neighbouring nodes only if it reputation value is higher than the threshold value i.e. this node must be in the white list. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no chance of re-joining the network until the entire network is reformed. This will decrease the efficiency and effectiveness of the network, low reputation value node is not allowed to participate in a network until network is reformed. We provided a solution that uses reputation with cache clearance process that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication. [10]

A formal study of MANET Security issues are presented by Nishu et al [19] which says MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and limited resource constraints etc. Security is not a single layer issue but a multi-layered issue. It requires a multi fence security solution that provides complete security spanning over the entire protocol stack.. They considered the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPsec are not applicable here. They looked at AODV in detail and developed a security mechanism to protect its routing information by developing a technique to periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol.

A formal study of MANET Security issues are presented by Nishu et al [19] which says MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and limited resource constraints etc. Security is not a single layer issue but a multi-layered issue. It requires a multi fence security solution that provides complete security spanning over the entire protocol stack.. They considered the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPsec are not applicable here. They looked at AODV in detail and developed a security mechanism to protect its routing information by developing a technique to periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol

Khalid at el [20] investigated some very common but challenging issues experienced by ad-hoc wireless communication. They have divided their studies into three sub-domains i.e. Security Models, Vulnerability in Current Protocols and Attacks. They Considered Security attacks as major issue of ad hoc networks which can be overcome up-to a level by adopting some proposed schemes. They explored the proposed methodologies and security schemes that guard against large number of attacks including DOS, Wormhole, Black hole and Flooding attacks. And concluded that these schemes are effective for detection attacks but still have limitations which raise questions on their usability. The protocols associated with MANETs require more research; especially reactive protocols may be trapped by intruders at the time of route discovery process.

## III. RESEARCH METHODOLOGY

In black hole attack, a node uses its routing protocol in order to broadcast itself for having the shortest path to the destination node or to the packet it wants to intercept. This black hole node promotes its availability of new active routes irrespective of checking its routing table. The availability of the black hole in the established path creates serious damages in packet transmission and reduces the through put of the network and also performance of the data transmission in the wireless sensor networks.

In the normal Dynamic Source Routing protocol, route discovery and route maintenance are the key process during the transmission between the source and destination nodes. Whenever source node has the data to send to the destination node, first it checks the route cache for the route to the destination and also verified status of the route whether it is unexpired route or expired route. If it has the unexpired route, then source node begins the data transmission to the destination nodes through its route specified intermediate notes. Otherwise perform the route discovery process by using RREQ (Route Request) packet which contains the source address and destination address. Route Requests are received by the intermediate nodes and sent the RREP (Route Reply) based on its availability of active routes to its adjacent nodes. The same process will be continued in the all intermediate nodes upto the period of RREQ reaches to destination node or intermediate node which has the route to destination in its route cache.

Route maintenance process is used to detect the availability of the path between the source node to destination node based on the routing table entry. Data packets are transferred from the source to destination nodes through intermediate notes in the route maintenance phase.

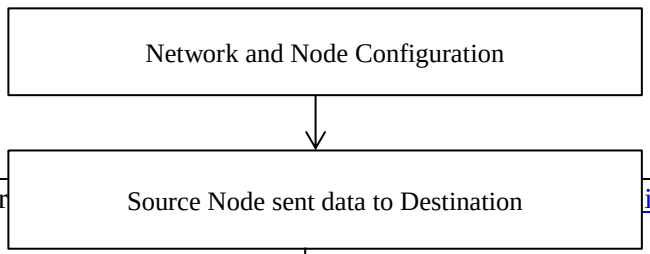

Fig. 3.1 The proposed Framework

In the Network and Nodes Configuration phase network and nodes are configured for the wireless sensor network formation using modified DSR based routing protocol with 6 nodes, 800 x 800 topology size.

After the configuration phase, source and destination nodes are initialized with data transmission initiation. Source node and Destination Node are randomly selected from the configured nodes.

The Route Discovery with Black Hole Detection Phase performed in three stages such as Route Request Stage, Route Reply Stage and Black Hole detection with Remove the node in routing table entry. In the route request, source node sent the request to the adjacent nodes and collects the reply from its adjacent nodes. Adjacent nodes are sent the route request to its adjacent nodes and get the reply from the nodes. This process will be continued upto destination node is obtained.

Black hole is detected based on the route reply from the adjacent nodes and its route reply status. It finds the nodes which are having active route and identified as the black hole. Those nodes are removed from the routing table entry.

In Route Maintenance Phase, source node transmits the data packets to the destination nodes through intermediate nodes based on the established route. During this packet transmission, each intermediate node's active routes are identified each time. Whenever intermediate node fails to transfer the packet to its adjacent nodes, automatically it produces the route error packet. Generated route error packets are sent to that intermediate node's previous node at the time of data can't be transmitted to its adjacent nodes. If Route error packet received by the source node then again it starts route discovery phase.

Route discovery, black hole detection with removal from the route table and route maintenance are the key process in this modified dynamic source routing protocol in the wireless sensor network simulation.

## IV. SIMULATION RESULTS

### SIMULATION SETUP

NS2 software has been used for the simulations of proposed algorithm due to its ease of node deployment and network set up. It has numerous built-in commands that help in node creation, simulation setup, implement modified DSR routing algorithm, detection of selfish nodes and creation of network animation and trace. With the help of NS2, critical analysis of results is achieved.

The simulation is conducted using Network Simulator – NS2. The simulation parameters are tabulated in Table.4.1

| **Simulation Parameter** | **Value** |
|---|---|
| Simulator | NS-2 (v.2.35) |
| Topology Size | 800 X 800 |
| Number of Nodes | 6 |
| Routing Protocol | DSR |
| Transmission Range | 250m |
| Channel Type | Channel/ Wireless channel |
| Interface Queue Length | 50 |

| | |
|---|---|
| Mac Type | Mac/802_11 |
| Interface Queue Type | Queue/Drop Tail/PriQueue |

Table 4.1 Simulation Parameters

The following metrics are used in this research work for the detection and prevention of the black hole attack with DSR routing protocol.

**PACKET DELIVERY RATIO**

The packet delivery ratio classifies the ability of the existing DSR and modified DSR protocol to discover routes. This ratio specifies the percentage of the data packets received by the destination node which are sent by the source node.

| Routing Algorithm | Packet delivery ratio in % |
|---|---|
| Existing DSR | 60 |
| Modified DSR | 87 |

Table 4.2 Packet Delivery Ratio of the DSR and Modified DSR

The above table reveals that the modified DSR without black holes shows the better performance than existing DSR with black holes in the packet delivery to the destination node

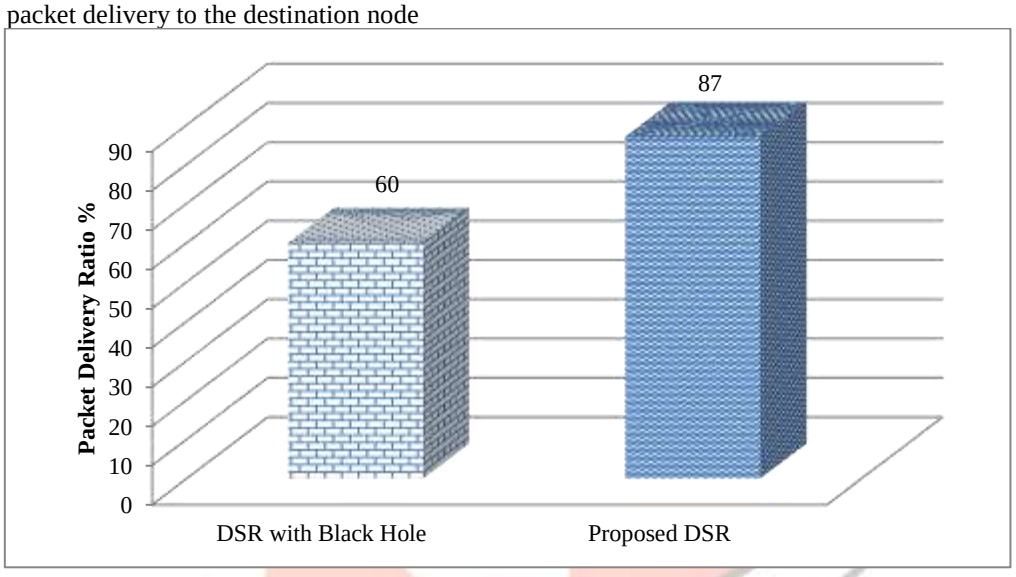


Chart 4.1 Packet Delivery Ratio of the DSR and Modified DSR

**END TO END DELAY**

This delay specifies the average delay between the sending of the data packet by the source node and its receipt at the destination node. Average delay includes route acquisition, buffering, black hole detection and process in the intermediate nodes.

| Routing Algorithm | Average Delay in ms (6 Nodes) |
|---|---|
| Existing DSR | 7 |
| Modified DSR | 5 |

Table 4.3. Average delay of the DSR and Modified DSR

The above table reveals that the modified DSR without black holes shows the better performance than existing DSR with black holes in the packet delivery to the destination node

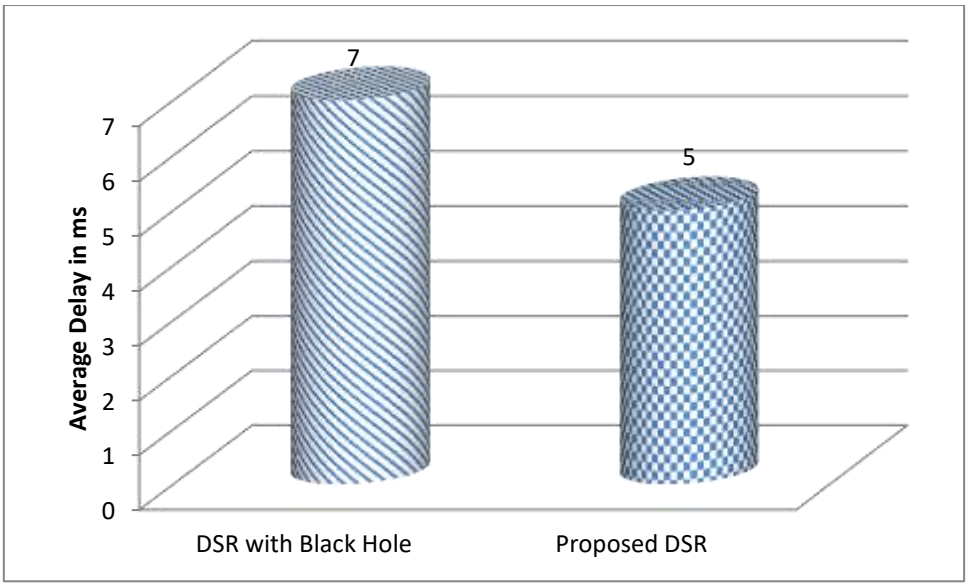


Chart 4.2. Average Delay of the DSR and Modified DSR

## CONCLUSION

In this research work, we addressed the problem of identifying and isolating black holes that refuse to forward packets in wireless ad hoc network. The impact of such nodes has been shown to be detrimental to network performance, dropping the network throughput and intensely increasing the end-to-end delay. To mitigate the problem of malicious packet dropping, we developed a comprehensive black hole detection and suppression system using modified DSR. Finally the implemented system detects and isolates the black holes and provides available alternative path to continue the packet forwarding thus keeping network stable and increasing the network performance and also network throughput.

## SCOPE FOR FUTURE ENHANCEMENT

In in the future we will try to find ways how these black holes can be avoided and adjusted routes automatically during packets transmission. This work can be extended to detect other types of attacks such as selfish nodes and other attacks which can help in improving performance of MANET.

## REFERENCES

1. Enrique Hernandez-Orallo et al. "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE transactions on Mobile Computing, vol. 14, no. 6, June 2015.
2. S. Buchegger et al., "Self-policing mobile ad hoc networks by reputation systems". Communications Magazine, IEEE, 43(7):101 – 107, July 2005.
3. S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks" Stanford University, Tech. Rep., 2003.
4. Khairu lAzmi Abu Bakar and James Irvine "Contribution Time-based Selfish Nodes Detection Scheme" ISBN: 978-1-902560-24-3 © 2010 PGNet.
5. M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz", On the effect of node misbehavior in ad hoc networks. In Proceedings of IEEE International Conference on Communications, ICC'04, pages 3759–3763. IEEE,2004.
6. C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs", International Journal of Wireless and Mobile Networks (IJWMN), 3(2):29–37, Apr 2011
7. C. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks", In Proceedings of Advanced Communication Technology (ICACT), volume 2, pages 1087 –1092, Feb. 2010.
8. Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks", In Proceedings of IEEEICC, volume 5, pages 3005 – 3009 Vol. 5, may 2005.
9. S. Marti, T. Giuli, K. Lai, and M. Bakar, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00), August 2000, pp. 255–265.
10. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," in IEEE Transactions on Mobile Computing, 2006, pp. 536–550.
11. Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks," in WCNC 2004, 2004.
12. S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol: (cooperative of nodes –fairness in dynamic ad hoc networks)," in Proc. IEEE/ACM Workshop on (MobiHoc'02), June 2002, pp.226–336.
13. P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in (CMS'02), September 2002.
14. K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005

15. S. Zhong, J. Chen, and Y. Yang, “Sprite: A Simple, Cheat-Proof, Credit- Based System for Mobile Ad-Hoc Networks”, Technical Report, Yale University, July 2002, pp. 1987-1997.
16. Wu, Lien-Wen, and Rui-Feng Yu, "A threshold-based method for sel_sh nodes detection in MANET."Computer Symposium (ICS), 2010 International IEEE, 2010.
17. Rajesh Sharma & Seema Sabharwal “Dynamic Source Routing Protocol (DSR)”, IJARCSSE, Volume 3, Issue 7, July 2013 pp. 239-241.
18. Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “A Survey of Reputation Based Schemes for MANET” 2010.
19. Renu Dalal1, Manju Khari and Yudhvir Singh “Different Ways to Achieve Trust in MANET” International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.
20. Santhosh Krishna B.V, Mrs. Vallikannu A.L “Detecting Malicious Nodes for Secure Routing in MANETS Using Reputation Based Mechanism” International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010.
21. Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, Fellow of IEEE and “Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks”, 2012.