Enhanced DSR protocol to analyze black hole attack in MANETs using NS2

R. Raghu[1], B. Nawaz[2], S. Sheyam Sundar[3], A. Shravan Kumar[4] & C. Sivakumar[5]

[1]Assistant Professor, Dept. of IT, Adhiyamaan College of Engineering (Autonomous), Hosur.

[2, 3, 4, 5] UG Scholars, Dept. of IT, Adhiyamaan College of Engineering (Autonomous), Hosur.

Abstract: *This Black-hole node aims to fool every node in the network that wants to communicate with another node. Detecting the malicious nodes in the network that intervenes black hole using the data control packet mechanism is a challenging task. In this paper, data control packets of Route Reply (RREP) is used to detect unsafe nodes. The RREP generator finds routes for each Route Request (RREQ). Throughput and packet delivery ratio decrease when the network is attacked by a black hole in the transmission of data because the malicious node absorbs or discards some of the packets. In this paper, the existing Dynamic Source Routing (DSR) protocol is modified with fake RREQ packets and a new Enhanced DSR protocol is proposed to analyze the black hole attack in Mobile Ad Hoc Network (MANET) using NS2. The new Enhanced DSR is compared in terms of Packet Delivery Ratio, Throughput, End-to-End Delay, and Packet Drop Ratio.*

Keywords: **MANETs, DSR, Black hole, and NS2.**

1. INTRODUCTION

This Mobile Ad hoc Network (MANET) which is also called Wireless Ad hoc Network (WANET) [1], usually has a routable networking environment. A set of mobile nodes is connected wirelessly in a self-configured network. As the network topology in MANET changes frequently nodes are free to move randomly. Rather than that, they cooperate to convey information between nodes that can't arrive at one another straightforwardly. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious about what data is sent over a MANET. MANET's energy is one of the most significant factor, as every node in the system has a restricted measure of energy; thus, we should work with effective components and conventions that maintain a strategic distance from any pointless energy [2] utilization. MANET associates nodes to one another utilizing a remote connection, where transmission capacity is viewed as a significant system property. The data transfer capacity of the remote connections is very much lower than that of the wired connections.

Attacks in MANET [3] The MANET comprises a dynamic set of self-organizing mobile devices or nodes that directly communicate with each other without any fixed infrastructure. Thus, nodes in MANET perform the tasks of both transceivers and routers to forward packets toward their destinations based on the employed routing protocol. Due to the dynamic nature of MANETs and their lack of fixed infrastructure, they are generally vulnerable to several types of attacks. These attacks include sinkhole, DoS (Denial of Service), DDoS (Distributed DoS), and blackhole attacks. Black hole attack [3] is a type of active attack that exploits the route reply message (RREP) feature of the routing protocol. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Fig. 1 shows an example of the impact of black hole attack in a network.

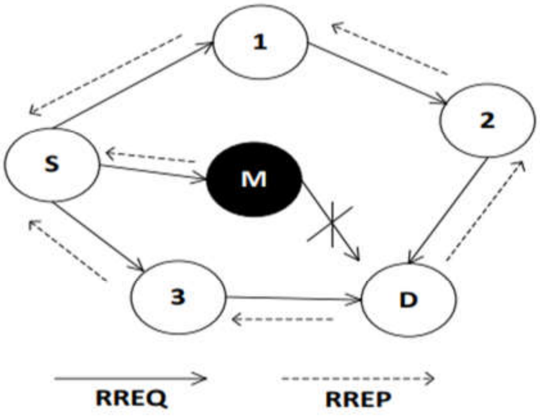

Figure 1 Example of Black hole Attack

Contribution of this paper:

- Enhancing the routing process using DSR.
- The Enhanced DSR is adopted to detect, analyze and overcome the impact of a black hole attack in MANET.
- In this paper enhanced DSR used to decrease the possibilities of passive attacks.
- Analyzing performance of enhanced DSR with respect to different parameters.

2. RELATED WORK

Yasin, A et al. [4], proposes an enhanced AODV by integrating a new lightweight technique that uses timers and baiting to detect and isolate single and cooperative black-hole attacks. During the dynamic topology changing, the suggested technique, Timer Based Baiting Technique (TBBT) enables the MANET nodes to detect and isolate the black-hole nodes in the network. The proposed TBBT integrates both timers and baiting techniques to enhance black-hole detection capability. The simulation results of the aforementioned technique showed that the Throughput, End-to-End Delay and Packet Delivery Ratio are very close to the native AODV.

Alem, Y et al. [5], introduced a solution that requires a source node to wait until an RREP packet appears from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node adjudicators that the route is safe. The main drawback of this solution is that it introduces time delay because it must wait until multiple RREPs turn up.

Kurosawa, S et al. [6], uses an anomaly detection scheme. The scheme uses a dynamic training method in which the training data is revised at regular time intervals. A multidimensional feature vector is defined to express the state of the network at each node. Each dimension is counted on every time slot. It uses the destination sequence number to detect the attack. The feature vector includes the number of sent out RREQ messages, the number of received RREP messages, the average of the difference of destination sequence number in each time slot between sequence number of RREP message and the one detained in the list. They calculate the mean vector by calculating some mathematical calculations. They evaluate the distance between the mean vector and the input data sample. If the distance is greater than some threshold value then there is an attack. The updated data set to be used for the next detection. Repeating this for time interval T anomaly detection is complete.

Tamilselvan, L et al. [7], proposed an improved solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses a loyalty table where every node that is participating is given a loyalty level that will offer reliability to that node. Any node having 0 values is considered as the malicious node and is removed from the network. The loyalty levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgment to the source; thereby the intermediate node's level will be increased. If no acknowledgment is received, the intermediate node's level will be decreased. The main drawback of this solution is the processing delay in the network.

Min, Z et al. [8], discussed an authentication mechanism to recognize black hole nodes in MANETs. An authentication mechanism is build based on the concept of the hash function, MAC, and PRF, which is used for checking the RREPs at source node to send the data packets. The projected mechanism removes the need for a PKI or other forms of authentication infrastructure, however, it needs to be discuses, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot fake a reply if the hash key of any node is to be released to all nodes.

Jalil, K et al. [9], have planned an ERDA solution to progress AODV protocol with minimum modification to the existing route discovery method recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When the RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet established by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is true, node S accepts the next RREP packet from other nodes to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. The current route entry in the routing table will be overwritten by the later RREP coming from other nodes. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. However, it cannot notice an obliging black hole attack.

Uke, S et al. [10], narrates the Physical and Data link layer attacks in WSN. It is addressing behavioral modeling of critical security attacks residing in the physical layer and data link layer of wireless sensor networks. UML gives the finest diagrammatic representation of any system which is best for developers. Our efforts to synchronize WSN with UML are discussed in the paper. The security attacks are modeled by using the state machine diagram of Unified Modeling Language (UML). This modeling of security attacks will help programmers to develop countermeasures.

] Zhang, X et al. [11], discussed a new detection method based on checking the sequence number in the Route Reply packets by making use of a new message created by the destination. In this method, when an intermediate node unicasts an RREP packet, the node also unicasts a newly defined control message to the destination node to request for the up-to-date SN. Upon receiving, the destination node unicasts a reply message to inform the source node of the up-to-date SN. This reply from the destination node permits the source node to verify if the intermediate node has sent a faked RREP message by checking if the SN in the RREP message is larger than the up-to-date SN. This method has more network overhead and time delay since the node in the network produces new packets.

Ochola, E et al. [12], analyses the black hole attack in MANET using both AODV and DSR. The simulation results showed that the performance of both AODV and DSR degrades in the presence of a black hole attack. Throughput and packet delivery ratio decrease when the network is attacked by a black hole because the malicious node absorbs or discards some of the packets. End-to-end delay is also reduced in the presence of a black hole attack because a malicious node pretends to have a valid route to a destination without checking the routing table, and therefore shortens the route discovery process.

TABLE 1 Comparison of existing protocols on various parameters.

Parameters	AODV	Enhanced DSR
Routing Type	Reactive	**Reactive**
Route Selection	Shortest & update path	Shortest & update path
Multiple Route	No	Yes
Routing structure	Flat structure	Flat structure
Multicasting	Yes	No
Congestion Handling	Yes	No
Route maintain in	Route table	Route cache
Updates transmitted to	Source	Source
QoS support	No	No
Periodic Broadcast	Yes	Yes
Advantages	Adaptable Higher bandwidth Lesser routing overhead Loop-free –Yes Uses Sequences number to keep the routing info updated.	Support multipath routing Less route discovery overhead Does not require any HELLO message exchange for route maintenance Loop-free -Yes
Disadvantages	Periodic Beaconing Takes more time to build a routing table Heavy Control Overhead	Scalability problem

Table1 depicts the comparison of existing protocols on various parameters. The AODV compared with proposed enhanced DSR in simulation section with various parameters.

Su, M et al. [13], proposed an intrusion detection system called Anti-Black hole Mechanism (ABM) in which the doubtful value of a node is estimated according to the amount of irregular difference between RREQs and RREPs spreader from the node; all nodes perform ABM. With the requirement that intermediate nodes are forbidden to reply to RREQs if an intermediate node is not the destination and never transmit RREQ for a specific route, but forward an RREP for the route, then its doubtful value will be raised in the nearby node's suspicious node table. When the doubtful value of a node goes ahead of the threshold, a Block message is broadcasted by the node to all other nodes in the network to separate the doubtful node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET. Table1 shows the comparison of existing protocols on various parameters. This comparison table deals with various similar parameters in the existing protocols. With this comparison, we are going to propose a new protocol with some modified features. There will be an improvement in the existing DSR protocol which is called Enhanced DSR.

3. PROPOSED WORK

The detection of a black hole attack in MANET is a critical task. To identify the black hole attack in MANET, DSR routing protocol is utilized and implemented. DSR is a loop-free, on-request (reactive) routing protocol that relies upon source routing. It is a self-organizing and self-configuring method. DSR doesn't utilize alternating updates as it computes routes when there is a need and after that keep up them. In this approach, the sender decides the total sequence of nodes through which the packet needs to travel, the sender attaches this route records in the packet's header. There are three phases of DSR protocol: -

- Route Discovery
- Route Reply
- Route Maintenance.

DSR gives incredible execution for routing in ad-hoc networks with no infrastructure or administration. It also reacts rapidly to changes in the network having very low overhead.

3.1 Working process of black hole attack detection

Network topology is the arrangement of the elements (links, nodes, etc) of a communication network. Network nodes are the points of connection of the transmission medium to transmitters and receivers. We can create a topology by interfacing the nodes in NS2. This protocol has two mechanisms- Route Discovery and Route Maintenance. The source route is needed when some node originates a new packet destined for some node by searching its route cache or initiate route discovery using ROUTE REQUEST and ROUTE REPLY messages. On detecting link break, DSR sends a ROUTE ERROR message to the source node for a new route. In figure 2, the step by step process of the detection of a black hole by Enhanced DSR is explained graphically. In the DSR protocol, fake RREQ packets are used to identify the malicious nodes. The reason for sending fake RREQ packets before initiating the actual routing process is to identify the malicious nodes in the network before the event of any damage. An acknowledgment scheme is used, where the data packets are only routed if and only if the source node receives the reply to the acknowledge packet sent by the source node. Thus, if the initial stage of sending the fake RREQ packets fails to identify the black hole node the proposed strategy of sending and receiving acknowledgment packet can identify the black hole nodes in the network.

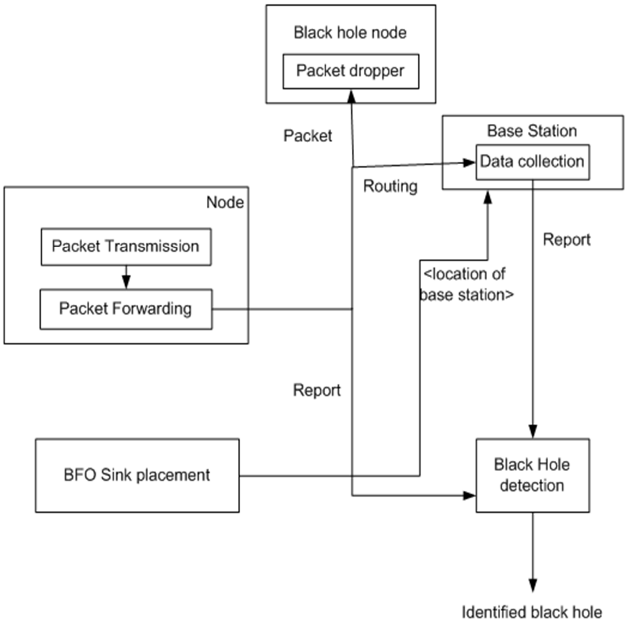

Figure 2 Architecture of Enhanced DSR

3.2 Route Discovery

In this process, the source node communicates the RREQ. Every node in network receives RREQ and verifies either it is destination or not. If it is not destination it forwards the RREQ to its directed node, otherwise reply is generated. An instance of the Route Discovery and Route Reply phase is represented in figure 3.

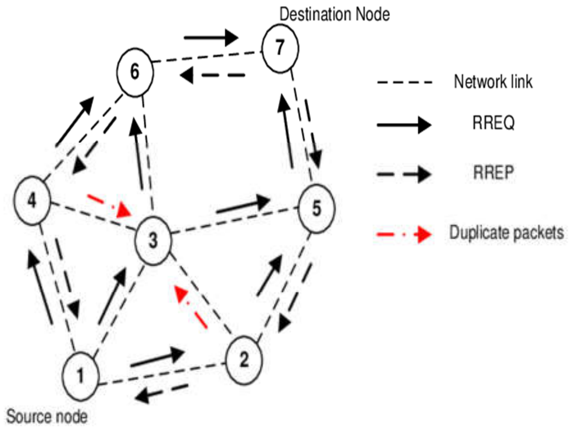

Figure 3 Route Discovery using RREQ and RREP

3.3 Route Reply

Intermediate nodes propagate the first RREP for the source. RREP utilizes stored switch sections to send reply. The route cache from RREP is copied to RREP and RREP is unicasted to source by following the header. The packet header contains the path to the source from destination.

3.4. Black Hole Creation and Detection

Black hole attack happens because of malicious nodes, which draws in the information by dishonestly promoting a new course to the goal. In the black hole attack, a malicious node utilizes its routing protocol to advertise itself for having the shortest path to its destination. This hostile node advertises its accessibility of fresh routes irrespective of scrutiny its routing table. In this attack, the attacker node continuously has the convenience of responding to the route request. In figure 4, the intermediate node 3, sends malicious RREP to the source node.

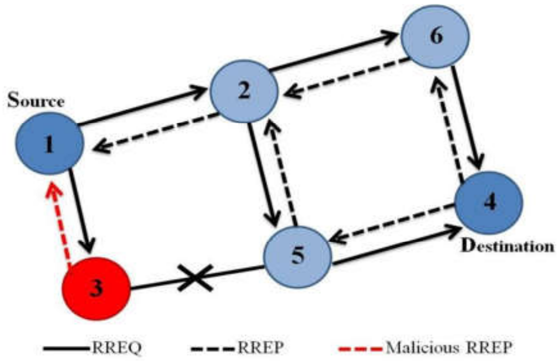

Figure 4 Black Hole node sending malicious RREP

4. RESULTS AND DISCUSSIONS

The simulation of the proposed model is done by using NS2. In the proposed system, we have enhanced the DSR protocol to detect and analyze the black hole attack in MANET. Considering the simulation of 100 nodes, the transmission of data packets is scheduled at a rate of 4packets/sec. The maximum speed of nodes will be 80m/s.

4.1 Simulation Environment

Parameter	Values
Simulator	NS-2.35
Mobility Model	Random Waypoint [13]
Simulation Time	500 seconds
Terrain Area	670m x 670m
Number of nodes and Black hole nodes	100 and 2
Packet Size	512 bytes
Routing Protocols & Traffic Type	DSR & CBR (UDP)
Transmission Rate & Maximum Speed	4 packets/sec & 20 – 80 m/s
Transmission Range and Beacon Interval	250m & 1sec

Table 2 Simulation Parameters

The simulation of the proposed model is done by using NS-2.35. The Mobility model follows a Random Waypoint. It is one of the most popular mobility models to evaluate MANET. In this model, the mobile nodes move randomly and freely without any restriction. The simulation time of the proposed model runs about 500 seconds. The terrain area is extended up to 670m x 670m. The simulation of 100 nodes is considered and analyzed in a Constant Bit Rate(CBR) traffic. In this simulation, the DSR protocol is modified and used to detect the black hole. The transmission of data packets is scheduled at a rate of 4packets/sec. Each packet size is about 512 bytes. A black hole node was set up to detect and analyze. The maximum speed of nodes will be 80m/s. The transmission range of the packets is 250m. The beacon interval in the transmission is set for 1 second. Table2 displays the simulation parameters considered.

4.2 Parameters

4.2.1 Packet Delivery Ratio (PDR)

Packet Delivery Ratio is the ratio of the data packets delivered correctly to the destinations. PDR is useful for calculating the packet loss. Equation (1) gives the arithmetic formula to calculate the PDR.

Packet Delivery Ratio = Σ Receive Packet / Σ Sent Packet (1)

The Packet Delivery Ratio is calculated by the ratio between the number of packets received at the destination to the number of packets sent from the source.

4.2.2 Throughput

Throughput is the number of received packets successfully at the recipient's side in a precise and it is represented in bps of the unit. Equation (2) provides a way to find the average throughput in terms of bits per second (bps).

Average throughput = Sum of packets successfully delivered-Total number of packets/Transmission time (2)

The Average Throughput can be found by the difference between the sum of the packets successfully delivered to each node and the total number of packets sent. The difference value should be divided by the transmission time.

4.2.3 Average end-to-end Delay

Time taken to deliver the packet from source to destination and the packet get delayed to transmit over a network is called routing delay. Equation (3) can be used to find the average delay in the transmission.

End to End Delay kpac =start time kpac – end time kpac (3)

Where 'kpac' is the start time when sending the packet 'pack' at node 'k' and end-time 'kpac', is the time when packet 'pac' is sent by node 'k' is received successfully at the destination node.

4.2.4 Packet Drop Ratio

Packet Drop Ratio is the ratio of the data packets not delivered correctly to the destinations. It is the ratio of the number of loss packets to the number of packets received. The Packet Drop Ratio can be found by equation (4).

Packet Drop Ratio = Σ Loss Packet / Σ Receive Packet (4)

The ratio between the number of packets lost to the number of packets received at the destination gives the Packet Drop Ratio.

4.3 Result

4.3.1 Packet Delivery Ratio

Packet Delivery Ratio in the proposed system has been improved than the existing system as more packets are received at the destination. As the black hole is detected quickly, more number of packets are sent to the destined node. Figure 5 depicts the comparison of PDR in AODV, DSR and Enhanced DSR.

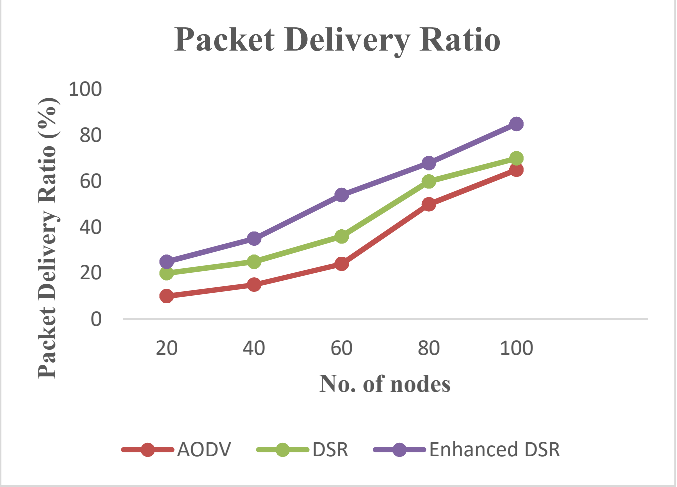

Figure 5 Packet delivery ratio

The PDR in the Enhanced DSR is higher than the other routing protocols considered. Because in AODV and DSR, there will be an inconsistency in the routing table.

4.3.2 Throughput

The throughput of the Enhanced DSR is high than that of other routing protocols in the sense of bits sent. The rate of the transmission is normalized as there is no malicious node in the route to the destination. The comparison of throughput in various protocols is depicted in figure 6.

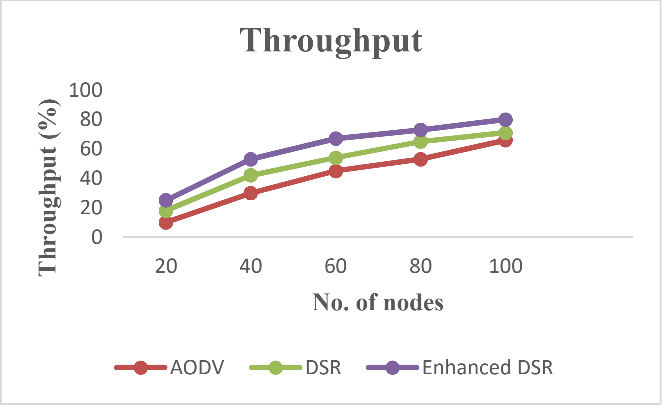

Figure 6 Throughput

The figure 6 shows that the throughput in Enhanced DSR is greater compared to AODV and DSR. As the performance of both the protocols degrades rapidly in the high-mobility environment, the Average Throughput is low.

4.3.3 Average End-to-End Delay

The End-to-End Delay is very much reduced because of the efficiency of the nodes in the network in Enhanced DSR. Figure 7 compares the Delay with the existing protocols. There is latency in the route discovery in both AODV and DSR. Therefore, there will be a delay in the transmission. But in the Enhanced DSR, the delay is much reduced than the other protocols.

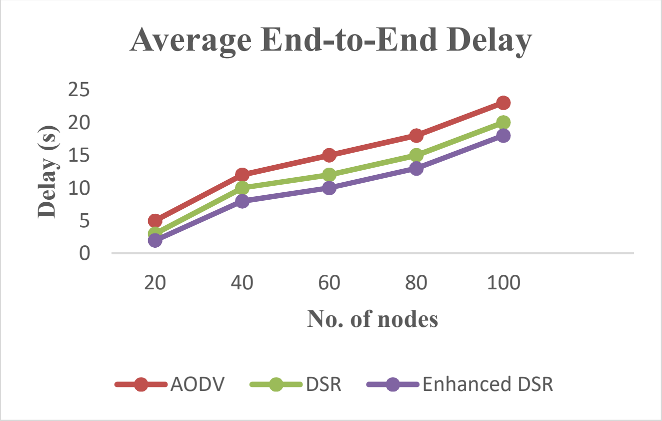

Figure 7 End to end delay

4.3.4 Packet Drop Ratio

The Packet Drop Ratio also reduced in the Enhanced DSR because most of the packets are dropped only at the destination node. A comparison of the Packet Drop Ratio on few protocols is represented in figure 8.

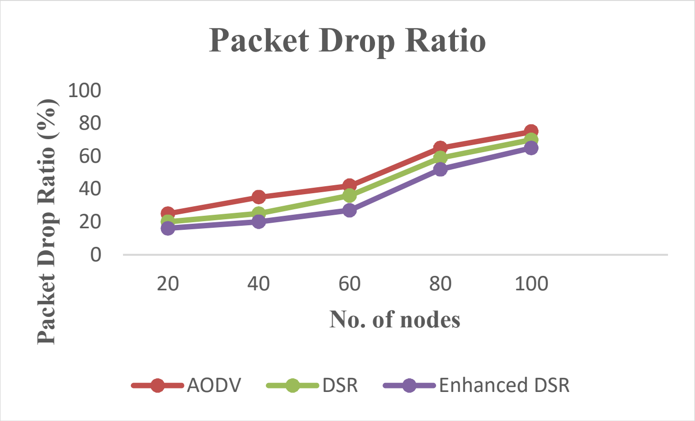

Figure 8 Packet Drop Ratio.

The periodic beaconing in the existing protocols leads to loss of packets. In the proposed Enhanced DSR, it is lowered.

5. CONCLUSION

Secure routing protocols are a crucial area towards the security of MANET. The routing solutions for conventional networks are not sufficient to work efficiently in an ad-hoc environment. In this dissertation, we have proposed a scheme to select a secure route for data forwarding. This technique will avoid the interception of messages through black hole nodes. We have compared our results with DSR routing protocol, the results showed that Secure DSR will avoid routing of packets through black hole nodes. The goal of this work is to provide a simple node-based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the NTM scheme. The model is simple, flexible and easy to be implemented.

REFERENCES

[1] Lokare, D., Kanthe, A. M., & Simunic, D. (2014). Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET. *International Journal of Computer Applications*, *88*(15).

[2] Badal, D., & Kushwah, R. S. (2015, December). Nodes energy aware modified DSR protocol for energy efficiency in MANET. In *2015 Annual IEEE India Conference (INDICON)* (pp. 1-5). IEEE.

[3] Chaudhari, H. C., & Kadam, L. U. (2011). Wireless sensor networks: security, attacks and challenges. *International journal of networking*, *1*(1), 4-16.

[4] Yasin, A., & Abu Zant, M. (2018). Detecting and isolating black-hole attacks in MANET using timer based baited technique. *Wireless Communications and Mobile Computing*, *2018*.

[5] Alem, Y. F., & Xuan, Z. C. (2010, May). Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. In *2010 2nd International Conference on Future Computer and Communication* (Vol. 3, pp. V3-672). IEEE.

[6] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *IJ Network Security*, *5*(3), 338-346.

[7] Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. *JNW*, *3*(5), 13-20.

[8] Min, Z., & Jiliu, Z. (2009, May). Cooperative black hole attack prevention for mobile ad hoc networks. In *2009 International Symposium on Information Engineering and Electronic Commerce* (pp. 26-30). IEEE.

[9]] Jalil, K. A., Ahmad, Z., & Manan, J. (2011). Mitigation of black hole attacks for aodv routing protocol. *International Journal of New Computer Architectures and their Applications (IJNCAA)*, *1*(2), 336-343.

[10] Uke, S., & Thool, R. (2016). UML based modeling for data aggregation in secured wireless sensor network. *Procedia Computer Science*, *78*(C), 706-713.

[11] Zhang, X., Sekiya, Y., & Wakahara, Y. (2009, March). Proposal of a method to detect black hole attack in MANET. In *2009 International Symposium on Autonomous Decentralized Systems* (pp. 1-6). IEEE.

[12] Ochola, E. O., Mejaele, L. F., Eloff, M. M., & van der Poll, J. A. (2017). MANET reactive routing protocols node mobility variation effect in analysing the impact of black hole attack. *SAIEE Africa Research Journal*, *108*(2), 80-92.

[13] Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, *34*(1), 107-117.