DOI: 10.21917/ijct.2019.0309

DCR-BASED HYBRID BLACK-HOLE AND GRAY-HOLE ATTACK DETECTION IN MANET

P. Rathiga[1] and S. Sathappan[2]
[1]*Department of Computer Applications, Navarasam Arts and Science College for Women, India*
[2]*Department of Computer Science, Erode Arts and Science College, India*

Abstract

Security of wireless network is a highly stimulating issue of today's life. The validation of all route messages is very problematic one due to the mobility and frequently modifying topology of the MANET. So in this paper, a DCR-based hybrid Black-hole/Gray-hole attack detection (HDCR) is proposed. In this approach, the malicious node attacks are identified by the Data to Control Packet Ratio value to avoid false detection. Data-to-Control Packet Ratio (DCR) is the ratio of number of data packet send by the node to number of control packet sent by the node. Each node will calculate the DCR value of its neighbour nodes in its own routing table. The maximum number of RREQ sent by any node is proportional to the DCR value of the node maintained by its neighbours. The experimental results compared the proposed HDCR detection with Hybrid detection method.

Keywords:

Data-to-Control Packet Ratio, HDCR, MANET, Hybrid Black-Hole or Gray-Hole Attack

1. INTRODUCTION

Generally, in MANET, route discovery process is a vulnerability of routing protocols which an attacker may exploit for performing a Black-hole attack [1] and Gray-hole attack [2]. A malicious node in the network can receive an RREQ message replies to source nodes by transmitting a fake RREP message that consists of desirable parameters to be selected for packet delivery to destination nodes. After promising (by transmitting a fake RREP for ensuring it has a path to a destination node) to source nodes that it will transmit data, a malicious node initiates to drop all the network traffic it receives from source nodes. This conscious dropping of packets by a malicious node can be detected by using monitoring nodes in the network.

However, some malicious nodes are not detected effectively and these malicious nodes can transmit the fake message to the other nodes by blocking the monitoring nodes in the network. Therefore, the hybrid Black/Gray-hole attack detection is enhanced by integrating network metric measurements. In this paper, the Data-to-Control Packet Ratio (DCR) is measured for removing malicious nodes from the network and also avoiding the false detection. This scheme requires whenever an attacker is identified, the type of attacker must be specified in the ALERT message packet. The ALERT packet consists of ID of identifying node, ID of malicious node, detection time and type of attacker. This modified version protocol includes new packets namely Further Request and Reply (FRREQ and FRREP) packets and Data-to-Control Packets (DCP). An attacker node must send a DCP packet if the packet is not for itself.

When a node receives a FRREQ packet from any other node, the node should transmit its next hop information as FFREP packet to the requesting node [3]. When a node receives a DCR packet, it should transmit the packet to its next hop if the packet is not for itself. If the packet is for itself, the node should retrieve the value stored in the *dropcount* field of packet. Then, the node should compare the retrieved *dropcount* value and its *rpcount* value.

Whenever a node gets a packet for transmitting to the other nodes, it creates an entry in its data routing table. It consists of details about the source and destination node, next hop, *fpcount*, *rpcount* and *dropcount*. In this table, *fpcount* and *rpcount* values corresponding to the destination nodes will be updated each time a packet is transmitted to this node and each time a packet is received by this node. Then, the node computes the *dropcount* for the next hop. The computed *dropcount* is compared against a predefined packet drop threshold. If *dropcount* is greater than the packet drop threshold, the next hop is identified as malicious [4]. The node terminates the data transmission temporarily.

After that, node creates a FRREQ packet and transmits it to malicious node, asking information of its next hop node in the current transmission path. The malicious node must reply the information of its next hop node. While receiving a FRREP packet, a node creates a DCP packet for transmission to the next hop node of malicious node. The DCP packet includes a value of *dropcount* which is set to current *fpcount* value corresponding to the malicious node. Then, DCP is transmitted to the next hop node via the malicious node. When DCP packet is received, a node extracts the *dropcount* value from the DCP packet and compares it with its own *rpcount* value.

Based on the DCP packets, DCR value is measured for each node and compared with the detection threshold to detect the malicious node. In this scheme, a node does not monitor each node in the neighbor, however promiscuously monitors only the next hop in the current routing path [5]. Every node confirms, packets transmitted to neighboring nodes are further being transmitted, provided the packet is not destined to that neighbor node. Each node monitors the transmission of data packets only. Before secure route discovery process, normal node sends less number of control packets and high number of data packets whereas it is vice versa after the route discovery process [6]-[11].

On the other hand, malicious node may send more number of control packets and less number of data packets during route discovery process. Thus, the estimation of DCR value is required for detecting malicious node in the network.

2. HYBRID BLACK OR GRAY-HOLE ATTACK DETECTION USING DCR MEASUREMENT (HDCR)

In the proposed HDCR approach, the malicious node attacks are detected by measuring the Data-to-Control Packet Ratio (DCR) of each node. DCR is defined as the fraction of number of data packets transmitted to the number of control packets

transmitted by the node. The malicious node detection is achieved by comparing the measured DCR value with the detection threshold. The detection process is performed in two phases such as route request phase and data transmission phase.

Initially, consider $K = \{k_1,k_2,\ldots,k_m\}$ number of nodes and L number of monitor nodes which is randomly initialized from K nodes. Each node in the network measures the *DCR* value as $DCR(k_1)$, $DCR(k_2)$,…, $DCR(k_m)$. For each node in the network, the DCR is measured as follows:

$$DCR_{k_i} = \frac{n_{dp}}{n_{RREQ}} \; ; \; i=1,2,\ldots,m \tag{1}$$

In Eq.(1), n_{dp} refers the number of data packets and n_{RREQ} refers the number of transmitted RREQ packets. Each node may collect the DCR value of its neighboring nodes such that, the DCR value of neighboring node is defined as follows:

$$N\left(DCR\right)_{k_i} = \left\{DCR_{k_i}, DCR_{k_j}\right\}; i, j = 1,2,...,m \text{ and } i \neq j \tag{2}$$

After that, the measured DCR values are sorted as follows:

$$DCR\left(k_i\right) = sort\left(N\left(DCR\right)_{k_i}\right) \tag{3}$$

The detection threshold value γ is also measured for detecting the malicious nodes. During route discovery process, the RREQ packets are transmitted from each node and the number of RREQ packets is higher for two conditions. The primary condition is that, initially the node does not contain any routing information so the RREQ packets are transmitted by the node for certain time duration. Another condition is that the number of RREQ packets is high while node mobility is high.

Hence, these two conditions are avoided by updating the DCR value at regular time duration and are denoted ast_{up}. The initial node behaviour at specific time duration is observed ast_{ob}. The DCR value is measured by each node after measuring the value of t_{ob} and the measured DCR value is updated for every t_{up} period. After that, the mean DCR value is computed and compared with the detection threshold value. In route request phase, the node is identified as malicious node, if the mean DCR value is less than the threshold value. In data transmission phase, the node is detected as malicious node, if the mean DCR value is higher than the threshold value.

Once the node is detected as malicious node, then the number of transmitting RREQ packets is limited. The false detection is reduced by updating the DCR value at regular time duration. Then, the monitor node updates the detected malicious node list U in routing table for advertising the node details to the network by using advertised message packets.

Algorithm:

Step 1: Consider K number of nodes
Step 2: Select L number of monitor nodes randomly
Step 3: Maintain the malicious node list U
Step 4: Initialize the detection threshold value
Step 5: //Route request phase
Step 6: Transmit RREQ packets by each node
Step 7: For each node do
Step 8: Measure *DCR* value $DCR(A)$, $DCR(B)$,…,$DCR(K)$ at t_{ob}
Step 9: End for
Step 10: Compute mean *DCR* value DCR_{M1}
Step 11: If ($DCR_{M1} < \gamma$) then
Step 12: Node=Malicious node
Step 13: End if //Data transmission phase
Step 14: For each data transmission do
Step 15: Measure *DCR* value at t_{up}
Step 16: Update the measured *DCR* value
Step 17: End for
Step 18: Compute mean DCR value DCR_{M2}
Step 19: If ($DCR_{M2} >$ *Threshold*) then
Step 20: Node=Malicious node
Step 21: End if
Step 22: Update malicious node list U
Step 23: Advertise the other nodes in the network
Step 24: End

3. PERFORMANCE EVALUATION

In this section, the performance of the proposed HDCR approach for MANET is evaluated in terms of Throughput, Packet Drop Rate, Packet Delivery Ratio and Normalized Routing Overhead and compared with hybrid Black/Gray-hole attack detection approach in the DSR protocol by using Network Simulator-2.34.

The performance metrics are evaluated for two types of simulation scenarios such as follows:

- **Scenario 1**: Fixed Mobility with varying number of malicious nodes.
- **Scenario 2**: Fixed number of malicious nodes with varying mobility of the nodes.

Scenario 1 refers the number of malicious nodes are varied from 2 to 10 and the mobility of the nodes are fixed as 50m/s. Scenario 2 denotes the number of malicious nodes are fixed as 10 and the mobility of the nodes are varied from 5m/s to 30m/s.

3.1 VARYING NUMBER OF MALICIOUS NODES WITH FIXED MOBILITY

3.1.1 Throughput:

The Throughput comparison values of hybrid detection and HDCR are shown in Table.1.

From the Table.1, it is noticed that the throughput of proposed HDCR is maximum while compared to the hybrid detection. For instance, when the number of malicious node is 8, the throughput for HDCR method is 16161Kbps which is higher than the hybrid detection (15890Kbps).

Table.1. Performance Comparison of HDCR Scheme in terms of Throughput (Kbps) under Scenario 1

No. of Malicious Nodes	Hybrid Detection	HDCR
2	16896	17930
4	16690	17330
6	16150	16759
8	15890	16161
10	15450	15793

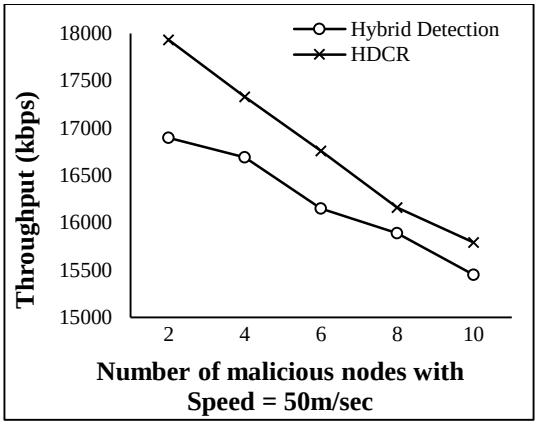

Fig.1. Comparison of HDCR Scheme in terms of Throughput under Scenario 1

The Fig.1 displays the proposed HDCR mechanism has better Throughput compared with the hybrid detection.

3.1.2 Packet Drop Rate:

The packet drop rate of hybrid detection method and proposed HDCR are given in Table.2.

Table.2. Performance Comparison of HDCR Scheme in terms of Packet Drop Rate (%) under Scenario 1

No. of Malicious Nodes	Hybrid Detection	HDCR
2	5.80	5.30
4	6.50	6.10
6	6.70	6.50
8	6.90	6.80
10	7.30	7.10

From the Table.2, it is observed that the packet drop rate of proposed method is minimum when compared to the existing method. For example, when the number of malicious nodes is 6, the packet drop rate for HDCR method is 6.50% which is less than the hybrid detection.

The Fig.3 portrays the examination of packet drop rate for the hybrid detection and HDCR approaches. Thus clearly demonstrates that the HDCR is efficient compared with the hybrid detection.

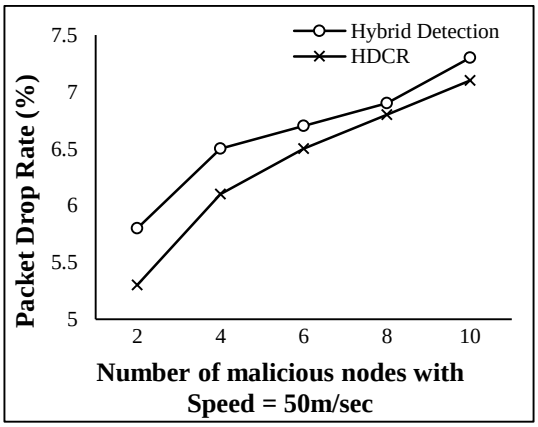

Fig.3. Comparison of HDCR Scheme in terms of Packet Drop Rate under Scenario 1

3.1.3 Packet Delivery Ratio (PDR):

The Table.3 shows the comparative study of proposed method HDCR method with existing method such as hybrid detection in terms of packet delivery ratio. It is observed that the Packet Delivery Ratio of proposed method is better than the existing method. For example, the packet delivery ratio for HDCR method is 82% for 2 malicious nodes whereas for hybrid detection is 77%.

Table.3. Performance Comparison of HDCR Scheme in terms of Packet Delivery Ratio (%) under Scenario 1

No. of Malicious Nodes	Hybrid Detection	HDCR
2	77	82
4	75	80
6	71	76
8	68	73
10	65	71

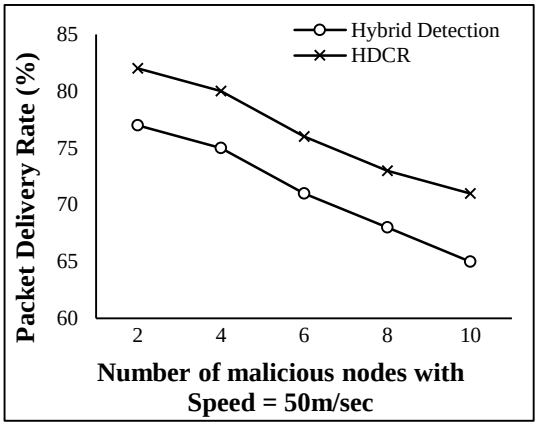

Fig.3. Comparison of HDCR Scheme in terms of Packet Delivery Ratio under Scenario 1

The Fig.3 depicts the analysis of the packet delivery ratio for the hybrid detection and HDCR approaches.

3.1.4 Normalized Routing Overhead:

The Table.4 describes the comparison values of normalized routing overhead for hybrid detection and HDCR are given in Table.4.

Table.4. Performance Comparison of HDCR Scheme in terms of Normalized Routing Overhead under Scenario 1

No. of Malicious Nodes	Hybrid Detection	HDCR
2	0.12	0.09
4	0.15	0.12
6	0.19	0.15
8	0.24	0.21
10	0.27	0.23

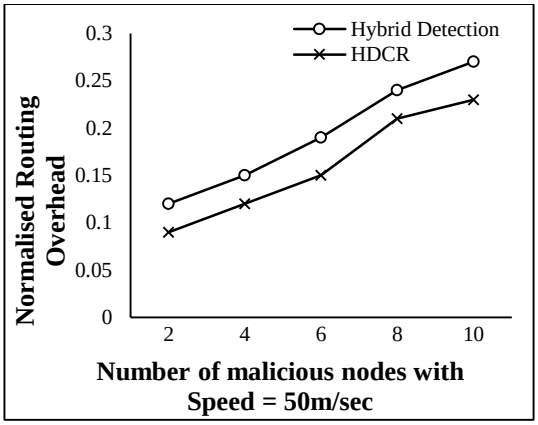

Fig.4. Comparison of HDCR Scheme in terms of Normalized Routing Overhead under Scenario 1

The Fig.4 describes the normalized routing overhead comparison of hybrid detection and HDCR approaches for mobility speed of the node is 50m/s. It shows that the proposed HDCR has better normalized routing overhead compared with the hybrid detection. For example, when the number of malicious node is 8, the normalized routing overhead for HDCR method is 0.21 which is less than the hybrid detection method.

3.2 VARYING THE MOBILITY OF NODES WITH FIXED NUMBER OF MALICIOUS NODES

3.2.1 Throughput:

The comparison values of throughput for hybrid detection and HDCR are given in Table.5.

Table.5. Performance Comparison of HDCR Scheme in terms of Throughput (Kbps) under Scenario 2

Speed (m/s)	Hybrid Detection	HDCR
5	17160	17453
10	16888	17251
15	16538	16984
20	16473	16756
25	16155	16435
30	16086	16167

It is observed that the throughput of proposed HDCR method is better than the Hybrid detection method. For example, the throughput for HDCR is 17453Kbps for node mobility is 5m/s whereas for hybrid detection is 17160Kbps.

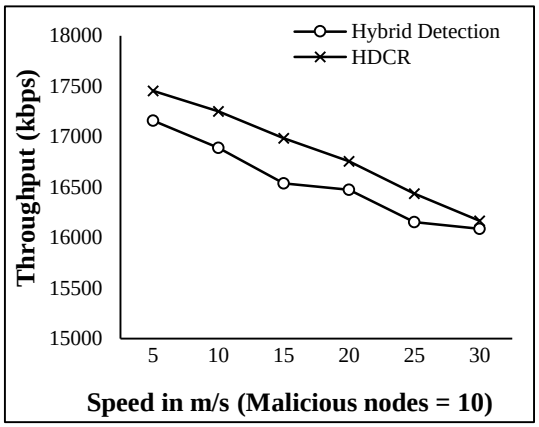

Fig.5. Comparison of HDCR Scheme in terms of Throughput under Scenario 2

The Fig.5 shows that the throughput comparison of hybrid detection and HDCR approaches. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the throughput values (Kbps) are taken in y-axis.

3.2.2 Packet Drop Rate:

The Table.6 shows the comparative study of proposed HDCR method with hybrid detection in terms of packet drop rate.

Table.6. Performance Comparison of HDCR Scheme in terms of Packet Drop Rate (%) under Scenario 2

Speed (m/s)	Hybrid Detection	HDCR
5	6.50	6.00
10	6.80	6.40
15	7.00	6.80
20	7.20	7.10
25	7.60	7.40
30	7.90	7.50

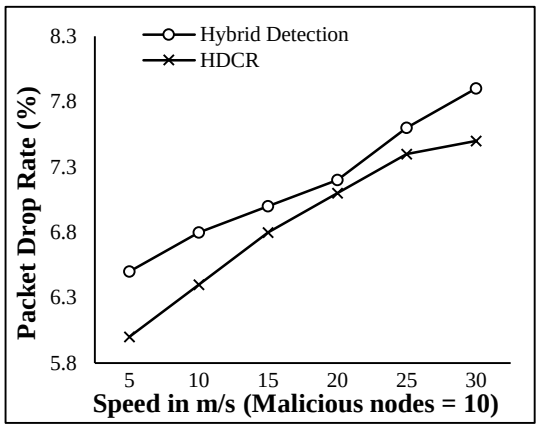

Fig.6. Comparison of HDCR Scheme in terms of Packet Drop Rate under Scenario 2

In the Fig.6, the mobility speed of nodes (m/s) is taken in x-axis and the packet drop rate values are taken in y-axis. It is observed that the packet drop rate of proposed HDCR is less when compared to the existing hybrid detection method. For example, when the node speed is 5m/s, the packet drop rate for HDCR method is 6% which is less than the hybrid detection.

3.2.3 Packet Delivery Ratio (PDR):

We study the packet delivery ratio for hybrid detection and HDCR for different speed of the malicious node. The results are captured in Table.7. It is identified that the packet delivery ratio of HDCR is high while compared to the hybrid detection method. For example, the packet delivery ratio of HDCR is 70% for node mobility is 20m/s which is higher than the hybrid detection method.

Table.7. Performance Comparison of HDCR Scheme in terms of Packet Delivery Ratio (%) under Scenario 2

Speed (m/s)	Hybrid Detection	HDCR
5	74	79
10	72	77
15	68	73
20	65	70
25	63	68
30	61	66

The Fig.7 shows that the packet delivery ratio comparison of hybrid detection and HDCR approaches. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the packet delivery ratio values (%) are taken in y-axitabs.

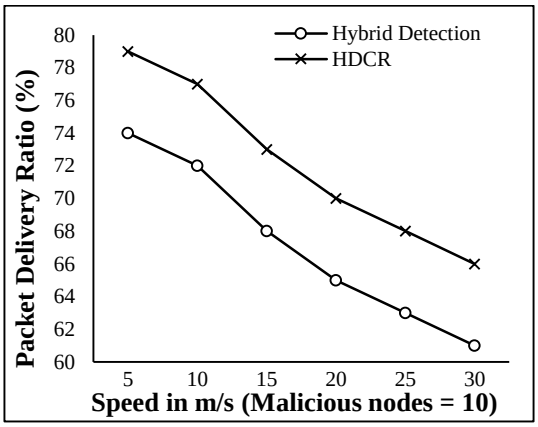

Fig.7. Comparison of HDCR Scheme in terms of Packet Delivery Ratio under Scenario 2

3.2.4 Normalized Routing Overhead:

The comparison values of normalized routing overhead for hybrid detection and HDCR are given in Table 8.

Table.8. Performance Comparison of HDCR scheme in terms of Normalized Routing Overhead under Scenario 2

Speed (m/s)	Hybrid Detection	HDCR
5	0.16	0.12
10	0.18	0.15
15	0.22	0.19
20	0.27	0.24
25	0.30	0.27
30	0.35	0.31

The Table.8 shows the comparative analysis of proposed HDCR with the hybrid detection in terms of normalized routing overhead. It is experienced that the normalized routing overhead of HDCR is less than the hybrid detection. Such as, the normalized routing overhead for HDCR is 0.31 for node mobility is 30m/s whereas for hybrid detection is 0.35.

The Fig.8 shows that the normalized routing overhead comparison of hybrid detection and HDCR approaches where the malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the normalized routing overhead values are taken in y-axis.

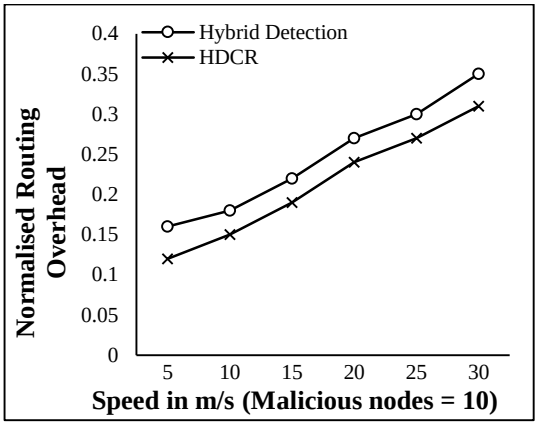

Fig.8. Comparison of HDCR Scheme in terms of Normalized Routing Overhead under Scenario 2

4. RESULT AND DISCUSSION

Here, DCR-based hybrid Black-hole/Gray-hole attack detection (HDCR) is proposed. In this approach, the malicious node attacks are identified by the Data to Control Packet Ratio value to avoid false detection. Data-to-Control packet Ratio (DCR) is the ratio of number of data packet send by the node to number of control packet sent by the node. Each node will calculate the DCR value of its neighbour nodes in its own routing table. The maximum number of RREQ sent by any node is proportional to the DCR value of the node maintained by its neighbours. For a malicious node, DCR value is less since it mostly sent route requests than the data packet and eventually the rate at which it can send RREQ will also be very less. Thus its maliciousness can be limited.

5. CONCLUSION

In this paper, the hybrid black-hole or gray-hole attack detection approach is improved by considering the network metric measurement such as DCR. Initially, DCR value for each node in the network is measured and then compared with the detection threshold for detecting the malicious node present in the routing path. Then, the detected Black-hole/Gray-hole nodes are removed from that routing path and a new path will be selected for the consecutive data packets transmission. Thus, the proposed HDCR detection approach is effectively detect the malicious nodes in the routing path effectively without any false detection. The experimental results proved that the proposed HDCR detection approach performs better than the other Black/Gray-hole detection approaches.

REFERENCES

[1] F.H. Tseng, L.D. Chou and H.C. Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks", *Human Centric Computing and Information Sciences*, Vol. 1, No. 4, pp. 1-16, 2011.

[2] Lalbihari Barik, "A Survey on Detecting Co-Operative Black Hole Attack on Multicast in Mobile Ad-Hoc Network", *International Journal of Current Engineering and Scientific Research*, Vol. 5, No. 11, pp. 149-155, 2018.

[3] Subhashis Banerjee and Koushik Majumder, "A Survey of Blackhole Attacks and Countermeasures in Wireless Mobile Ad-hoc Networks", *Proceedings of International Conference on Security in Computer Networks and Distributed Systems*, pp. 396-407, 2012.

[4] H. Khattak and Nizamuddin, "A Hybrid Approach for Preventing Black and Gray-Hole Attacks in MANET", *Proceedings of 8th International Conference on Digital Information Management*, pp. 1-12, 2013.

[5] V.A. Hiremani and M.M. Jadhao, "Eliminating Co-Operative Black-Hole and Gray-Hole Attacks using Modified EDRI Table in MANET", *Proceedings of International Conference on Green Computing, Communication and Conservation of Energy*, pp. 944-948, 2013.

[6] T. Lathies Bhasker, "A Scope for MANET Routing and Security Threats", *ICTACT Journal on Communication Technology*, Vol. 4, No. 4, pp. 840-848, 2013.

[7] A. Dhaka, A. Nandal and R.S. Dhaka, "Gray and Black-Hole Attack Identification using Control Packets in MANETs", *Procedia Computer Science*, Vol. 54, pp. 83-91, 2015.

[8] A. Dorri, S. Vaseghi and O. Gharib, "DEBH: Detecting and Eliminating Black Holes in Mobile Ad Hoc Network", *Wireless Networks*, Vol. 24, pp. 2943-2955, 2016.

[9] A. Dorri and S. Reza, "A Fuzzy Congestion Controller to Detect and Balance Congestion in WSN", *International Journal of Wireless and Mobile Networks*, Vol. 7, No. 1, pp. 137-145, 2015.

[10] R.H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV based MANETs", *Proceedings of 3rd International Conference on Advanced Computing and Communication Technologies*, pp. 254-260, 2013.

[11] M. Mohanapriya and I. Krishnamurthi, "Modified DSR Protocol for Detection and Removal of Selective Black Hole Attack IN MANET", *Computers and Electrical Engineering*, Vol. 40, No. 2, pp. 530-538, 2014.