International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Effective Secure Mechanism using Fuzzy Hybrid DCR Technique for MANET

P. Rathiga, S. Sathappan

Abstract*: Due to various Denial-of-Service (DoS) attacks like blackhole and grayhole attacks, Mobile Ad-Hoc Networks (MANET) performance is degraded rapidly. These attacks have been detected and prevented separately by different techniques. In earlier research, hybrid black/grayhole attack detection was proposed in which blackhole and grayhole attacks were detected and prevented simultaneously based on the detection threshold. However, some malicious nodes are still present in the network by faking the threshold value and forwarding the fake message to the other nodes. Therefore, the hybrid black/grayhole 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. In addition, fuzzy-based mobility and traffic measurement is integrated with a hybrid DCR detection technique for removing malicious node links. Moreover, the optimal path for packet transmission is selected by measuring the queue delay based on fuzzy logic optimization. Finally, the efficiency of the proposed hybrid blackhole/grayhole attack detection technique is illustrated through the simulation results based on the throughput, packet drop rate, packet delivery ratio and routing overhead.

***Keywords*: MANET, Denial-of-service, Blackhole attack, Grayhole attack, Data-to-control packet ratio, Fuzzy logic.**

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a type of wireless ad-hoc networks, which contains the self-configuring mobile devices and independently travels in any direction that provides the variations in the communication link about other devices recurrently. This type of network is used in various applications such as defense operations, emergency operations. In a MANET, each node acts as a host as well as a router. The cooperation is required by each node with respect to the other node for forwarding the data packets during receiving packets. However, the major issue in MANET is the constraints on the security of the routing and network topology. Since the collaboration of malicious nodes, the routing process is affected. The lack of infrastructure along with the dynamic network topology of MANET provides highly vulnerable to the routing attacks namely blackhole and grayhole attacks.

Black hole attack also known as packet drop attack is the malicious node attack in the network in which the receiving or transmitting packets are discarded silently without informing the source node. It is one of the types of Denial-of-Service (DoS) attack where the router drops the packets instead of transmit them. The detection and prevention of a blackhole attack are the most complex issue since the packets are discarded frequently from the lossy network. The malicious node waits for the neighbor nodes in order to generate the Route Request (RREQ) packet. While the malicious nodes receive the RREQ packet, it directly transmits the false Route Reply (RREP) packet with modified higher sequence numbers. Therefore, the source node considers that the new path is generated towards the destination node. Thus, the source node discards the RREP packets from other nodes and transmits the packet through the malicious node. Then, the packets from the source node are discarded by the malicious that does not allow it to forward to the destination or other nodes.

The blackhole node has two properties such as the node enters in Ad-hoc On-demand Distance Vector (AODV) protocol by representing itself as a valid path for destination and it starts receiving the packet from the valid nodes and also discards the packets which contains the valuable information. The blackhole attacks are classified into two types such as single blackhole attack and cooperative blackhole attack. More number of malicious node attacks is established in the cooperative blackhole attack whereas in single blackhole attack, only one malicious node attack is established on the path, whereas. The grayhole attack is similar to the blackhole attack, but sometimes it forwards the packets like other normal nodes in the network. Grayhole attack may selectively discard the packets without any certainty. It may discover the malicious activities based on dropping the data packets or transmitting the data packets normally from other nodes at certain time duration.

Different techniques are developed for detecting and preventing the blackhole and grayhole attacks. These collaborative attack detection techniques are utilized for detecting a blackhole or grayhole separately either in parallel or serial manner [1]. In previous research, hybrid black/grayhole detection and prevention technique is proposed for simultaneously detecting both attacks in Dynamic Source Routing (DSR) for MANET based on the two different detection threshold values.

Manuscript published on 30 September 2019
* Correspondence Author
Dr. P. Rathiga*, Department of Computer Applications, Navarasam Arts & Science College for Women, Erode, India. Email: rathigaphd@gmail.com
Dr. S. Sathappan, Department of Computer Science, Erode Arts & Science College, Erode, India. Email: sathappanerode@gmail.com

Initially, the malicious nodes are detected by comparing the first detection threshold value with the information distance metric value of each node in the network. Then, the blackhole or grayhole attacks which are performed by the detected malicious node are detected by comparing the second detection threshold.

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, in this paper, the hybrid blackhole/grayhole detection is improved by computing the Data-to-Control packet Ratio (DCR) value. The malicious node attacks are detected by comparing the DCR value of each node with the threshold value. However, due to high mobility of the nodes some messages are forwarded through the malicious nodes, which are present in the routing path. Therefore, the routing path free from malicious nodes is selected based on the fuzzy-based mobility and traffic measurements. Moreover, the nodes with less DCR value are required to be further analyzed for avoiding the false identification. Hence, the hybrid detection technique is further improved by measuring the queuing delay which is utilized for improving the packet delivery ratio and the node failure is avoided by selecting the optimal path in which no malicious nodes are detected.

The remainder of the article is organized as follows: Section 2 provides the different blackhole/grayhole attack detection techniques. Section 3 describes the proposed hybrid blackhole/grayhole attack detection technique using DCR, mobility and traffic measurement. Section 4 illustrates the performance evaluation of the proposed technique compared with other techniques. Section 5 concludes the research work.

II. LITERATURE SURVEY

An enhanced modified ad-hoc on-demand distance vector (EMAODV) technique [2] was proposed based on the extension of AODV by including control packets such as secure reliable route discovery request (SRRD_REQ) and secure reliable route discovery reply (SRRD_REP) and threshold value for preventing the collaborative attacks in mobile ad-hoc networks. Based on these additional packets, the malicious nodes were detected and prevented during route discovery process. However, routing overhead was increased for large size of MANET.

The detection and removal mechanism [3] was proposed for blackhole and grayhole attacks. In the proposed mechanism, the blackhole and grayhole attacks were prevented by maintaining the extended data routing information (EDRI) table at every node including with the AODV protocol routing table. The malicious nodes were detected by the fields of this table and the gray behaviour was accommodated by maintaining the history of previous malicious instances. In addition, different packets were utilized such as refresh packet, renew packet, BHID packet, further request, and further reply packets including with RREQ and RREP. However, the non-consecutive cooperating nodes were not identified and its usage effectiveness was less.

A cooperative bait detection technique [4] was proposed for defending against collaborative attacks in MANET. Based on cooperative bait detection scheme (CBDS) the problem of dynamic source routing (DSR) protocol was resolved by integrating the proactive and reactive defense infrastructures. The reverse tracing technique was implemented by CBDS for achieving the objective the proposed scheme. However, the security mechanisms were required for routing the packets.

An energy efficient technique [5] was proposed for preventing the grayhole and blackhole attacks in wireless sensor networks by selecting the optimal cluster head. In this technique, the secure routing path was generated from source node to the sink node which is utilized for eliminating the malicious node during data transmission. Furthermore, the proposed technique was utilized for preventing the compromised node to become cluster head during cluster head selection process. However, the communication overhead and bandwidth consumption were not reduced.

A cooperative blackhole and grayhole attack detection [6] was proposed based on the Modified Extended Data Routing Information (MEDRI) table in MANET. MEDRI table at each node along with AODV routing table was utilized for detecting the nodes which are affected by the cooperative attacks in MANET. Moreover, the detected cooperative blackhole or grayhole attacks were removed by implementing Negative Acknowledgement (NACK). However, the previous malicious node's history was needed to maintain for discovering the secure path.

The data forwarding model [7] was proposed for detecting the malicious node in MANET. Initially, different legitimate packet discard situations were modelled and an anomaly-based Intrusion Detection System (IDS) was proposed by using enhanced windowing technique. Then, the collection of the selected cross-layer features were achieved by the proposed IDS methodology. By using the proposed IDS system, the dropping attacks were detected. However, the network overhead was high and secure transmission was not considered.

The blackhole attack detection in MANET [8] was developed by using biology-inspired technique. An Ad-hoc On-demand Distance Vector (AODV) routing protocol was modified by using Ant Colony Optimization (ACO) algorithm. The pheromone value of each ant was computed at every node based on the forwarding ratio at node. The Ant Colony based Routing Algorithm (ARA) was effectively utilized in MANET for providing the secure routing path table without any malicious node and reducing the routing overhead. However, this technique was suitable for detecting only one attack.

A hybrid swarm intelligence algorithms [9] were proposed for improving the blackhole attack detection in MANET. A Hybrid Glow-worm Swarm Optimization (HGSO) algorithm with Artificial Fish Swarm Algorithm (AFSA) was proposed. The proposed hybrid algorithm was utilized for fast convergence process with reduced routing complexity. The security algorithm was also utilized for avoiding blackhole attacks by using encryption technique. However, the proposed method was not suited for detecting more than one attack.

The removal of selective blackhole attack [10] was investigated in Dynamic Source Routing (DSR) protocol. Here, the removal of blackhole attack was described based on the alarm system using in the network by updating the malicious node detection in network and the packets were forwarding to its upstream and downstream nodes. Therefore, the malicious nodes were avoided by the nodes and the data were forwarded through the selected path. However, the routing overhead was not considered.

The trust assurance based mechanism [11] was proposed for detecting grayhole attacks in MANET. In this mechanism, the grayhole attack was detected by using the trust algorithm which is based on the uncertain reasoning. The uncertain reasoning was provided for computing the trust value. In addition, hand information was utilized for computing trust value indirectly. The trust value was assured based on the detection and removal of the malicious node from the network. However, the normalized routing head was slightly high.

A Modified Cooperative Bait Detection Scheme (MCBDS) [12] was developed by improving CBDS technique for grayhole and blackhole attacks in MANET. The proposed technique was utilized for reducing the false positive rate and improving the accuracy of the detection process. In addition, the processing load and routing packets size were also reduced by eliminating some operations and transmitted data in the network. However, the network performance improvement was still required.

An efficient Crypto-key based Black Hole Detection and Avoidance Protocol (CBHDAP) [13] was developed for detecting and eliminating the blackhole attacks in MANET effectively. Diffie-Hellman based key agreement blackhole detection algorithm was applied for generating the group of key. Before initiating the transmission, the nodes in the routing were validated. By considering the network metrics such as route reply, hop count, packet delivery ratio, the blackhole attacks were removed during data transmission. However, the detection probability was less.

Grayhole attack detection and removal technique [14] was proposed in MANET. An algorithm was proposed for detecting and removing the grayhole attacks in the networks based on the dynamic credit based mechanism which utilizes the AODV routing protocol. The credit value was measured instead of the destination sequence number for detecting grayhole attacks. However, the secure routing and routing overhead were not considered.

A cooperative blackhole and grayhole attack detection and removal technique [15] was proposed in mobile ad-hoc networks. Initially, the misbehaving of packet forwarding was addressed and a technique was proposed for detecting and removing both blackhole and grayhole attacks. In this technique, the total data traffic was separated into the small sized blocks. Hence, the malicious nodes were detected between two blocks based on end-to-end checking effectively and the detected malicious nodes were eliminated from the routing. However, the performance of the proposed technique was not analyzed.

MRAODV protocol [16] was proposed based on the Reliable-AODV protocol for detecting blackhole and grayhole attacks in AODV based MANET. The attack detection problems were resolved by this technique by means of isolating the blackhole and grayhole attacks during data transmission. The normalized routing overhead was reduced based on the reduction in number of forwarded reply packets which are transmitted by adversaries. However, the detection performance was degraded due to the increased delay.

III. PROPOSED METHODOLOGY

In this section, the proposed improved hybrid black/grayhole attack detection using different network metrics are explained. Initially, the hybrid black/grayhole attack detection technique [17] is discussed. In hybrid black/grayhole attack detection, number of nodes is deployed in DSR protocol and the monitor nodes are initialized for gathering the packet flow information from neighboring nodes. The attacker node transmits the RREP packets with high sequence number for route discovery process, while source node transmits the RREQ packets. The collection of packet flow information by the monitor nodes is utilized for computing the information distance metric for all nodes. Then, the computed distance metric value is compared with two detection thresholds in order to detect the malicious nodes and the attack is whether blackhole or grayhole.

A. Hybrid Black/Grayhole Attack Detection using DCR (HDCR) Measurement

In the proposed HDCR technique, 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 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 $DCR(A), DCR(B), \ldots, DCR(K)$. 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 as t_up. The initial node behaviour at specific time duration is observed as t_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:

1. Consider K number of nodes
2. Select L number of monitor nodes randomly
3. Maintain the malicious node list U
4. Initialize the detection threshold value γ

//Route request phase

5. Transmit RREQ packets by each node
6. For each node do
7. Measure DCR value $DCR(A), DCR(B), \dots, DCR(K)$ at t_ob
8. End for
9. Compute mean DCR value DCR_{M1}
10. $If\,(DCR_{M1} < \gamma)$ then
11. Node=Malicious node
12. End if

//Data transmission phase

13. For each data transmission do
14. Measure DCR value at t_up
15. Update the measured DCR value
16. End for
17. Compute mean DCR value DCR_{M2}
18. $If\,(DCR_{M2} > Threshold)$ then
19. Node=Malicious node
20. End if
21. Update malicious node list U
22. Advertise the other nodes in the network
23. End

B. Fuzzy-based Mobility and Traffic Measurement based Hybrid DCR Black/Grayhole Attack Detection (FMTMHDCR) Technique

In HDCR technique, still some packets are transmitted through the malicious nodes which are not removed from the routing path due to the mobility of nodes. Hence, the malicious nodes are effectively removed from the routing path by using fuzzy-based mobility and traffic measurements. The mobility and traffic factors are compared with the detection threshold for detecting and removing the malicious node from routing path.

Consider K number of nodes and L number of randomly initialized monitor nodes. Once transmission is initiated, DCR value is computed by each node along with the mobility and traffic. Based on the measurement of link pause time lp_t the mobility is computed which helps to identify the link failure in the path. In addition, the computation of queue length $qlen$ of each node in the network helps to determine the traffic. After that, the computed traffic and mobility values are converted into the fuzzy membership function for detecting the malicious node in the network effectively. In addition, fuzzy logic technique is utilized for selecting the routing path which is free from the malicious node and with minimum link failure and maximum queue length.

Algorithm:

1. Consider K number of nodes
2. Select L number of monitor nodes randomly
3. Maintain the malicious node list U
4. Initialize the detection threshold value γ
5. Transmit RREQ packets by each node
6. For each node, do
7. Calculate DCR value
8. Compute link pause time, lp_t
9. $If\,(lp_t > \gamma)$ then
10. Mobility=High
11. Else
12. Mobility=Less
13. End if
14. Compute queue length, $qlen$
15. $If\,(qlen < Threshold)$ then
16. Traffic=Less
17. Else
18. Traffic=High
19. End if
20. End for
21. Initialize the fuzzy membership variables
22. Obtain the fuzzy membership functions
23. Construct the rule base
24. {
25. Rule1: Mobility=High & Traffic=Less
26. Rule2: Mobility=High & Traffic=High
27. Rule3: Mobility=Less & Traffic=Less
28. Node=Malicious node
29. Remove the malicious node from U
30. Reject the routing path
31. Transmit the packets from neighboring routing path
32. Rule4: Mobility=Less & Traffic=High
33. Node=Normal node
34. Select the routing path
35. }
36. End

C. Fuzzy-based Queue Delay Measurement based FMTMHDCR Black/Grayhole Attack Detection (FMQTMHDCR) Technique

In HDCR and FMQTMHDCR techniques, the nodes with less DCR, mobility and traffic values are needed for further analysis in order to avoid the false identification effectively. Hence, the detection and removal of malicious node attacks are enhanced by adding fuzzy-based queue delay measurement with mobility, traffic and DCR values. Due to mobility of the nodes, the packet delivery ratio may be decreased. The packet delivery may be reduced by increasing the queuing delay which occurs during high traffic. Hence, the proposed queue delay measurement checks the reason for failure of the data packets during transmission. If the reason of packet failure is valid, then the node is considered to be normal otherwise the node is malicious node.

The major objective of this FMQTMHDCR technique is to discriminate the normal node with malicious node by using packet delivery ratio.

Consider K number of nodes and L number of monitor nodes which is randomly initialized from K nodes.

Each node computes their DCR value as well as mobility and traffic during transmission. For each node in the network, queuing delay $qdelay$ is computed for identifying the congestion level and traffic level. In addition, packet flow of each node pf is also measured for analyzing the packet delivery ratio (PDR). Then, the computed values are fuzzified and de-fuzzified in order to identify the malicious nodes as well as choose the optimal routing path for transmitting the data packets. If the node in selected routing path is detected as malicious node, then the selected path is removed form the routing table and the optimal routing path from other available paths is selected as routing path for transmission. Thus, the proposed FMQTMHDCR technique can be utilized for detecting and removing the malicious nodes from the routing path for data packet transmission in MANET efficiently.

Algorithm:

1. Consider K number of nodes
2. Select L number of monitor nodes randomly
3. Maintain the routing table list R
4. Initialize the detection threshold value γ
5. Transmit RREQ packets by each node
6. For each node do
7. Calculate DCR value, link pause time and queue length
8. Calculate queuing delay, $qdelay$
9. $If\,(qdelay > \gamma)$ then
10. Congestion=High & Traffic=High
11. Else
12. Congestion=Less & Traffic=Less
13. End if
14. Analyse the packet flow, pf
15. $If\,(pf < \gamma)$ then
16. PDR=Less
17. Else
18. PDR=High
19. End if
20. End for
21. Initialize fuzzy membership functions
22. Construct the fuzzy rule base
23. {
24. Rule1: PDR=High & Traffic=High
25. Rule2: PDR=Less & Traffic=High
26. Node=Malicious node
27. Remove the routing path
28. Choose optimal routing path from other available paths
29. Rule3: PDR=High & Traffic=Less
30. Rule4: PDR=Less & Traffic=Less
31. Node=Normal node
32. Transmit the packets from selected routing path
33. }
34. End

IV. PERFORMANCE EVALUATION

In this section, the performance of the proposed hybrid black/grayhole attack detection is evaluated based on the network parameters such as throughput, packet drop rate, packet delivery ratio, and normalized routing overhead. The simulation parameters are given in Table 1.

Table 1: Simulation Parameters

Simulator	NS-2.34
DoS attack	Black/Gray-hole attack
Channel Type	Channel/Wireless Channel
Antenna Type	Antenna/Omni Antenna
Radio Propagation model	Propagation/Two Ray Ground
Link Layer type	LL
Interface queue type	Queue/ Drop Tail / PriQueue
MAC type	MAC/802.11
Protocol studied	DSR
Simulation area	1000*1000
Trace format	New wireless format
Node movement model	Random waypoint
Traffic type	CBR (UDP)
CBR rate	50 Kbps
Data Payload	512 bytes/packet
Number of nodes	50
Malicious nodes	10
Speed	50m/sec

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

- Scenario 1: Varying the number of the malicious nodes with fixed mobility.
- Scenario 2: Varying the mobility of the nodes with fixed number of the malicious nodes.

A. Performance Metrics

- Throughput: The amount of forwarded data packets over a time period is known as throughput and its unit is Kilobits per second (Kbps).

$$Throughput = \frac{Number\ of\ transmitted\ packets}{Time\ taken}$$

- Packet drop rate: The fraction of the amount of dropped data packets at the destination to the total amount of generated data packets at the source is known as packet drop rate.

$$Packet\ Drop\ Rate = \frac{Number\ of\ dropped\ packets\ at\ destination}{Total\ number\ of\ packets\ generated\ at\ source}$$

- Packet delivery ratio: The fraction of the total amount of data packets received at the destination to the total amount of forwarded packets from the source is called as packet delivery ratio.

$$Packet\ Delivery\ Ratio = \frac{Total\ number\ of\ packets\ received\ by\ destination}{Total\ number\ of\ packets\ sent\ by\ source}$$

- Normalized routing overhead: The fraction of the amount of routing packets like RREQ and RREP forwarded per data packet is known as normalized routing overhead.

$$Routing\ Overhead = \frac{Total\ number\ of\ routing\ packets\ transmitted}{Total\ number\ of\ data\ packets\ received}$$

B. Analysis of Fixed Mobility with Varying Number of Malicious Nodes

The comparison values of throughput for existing and different proposed approaches are given in Table 2.

Table 2: Comparison of Throughput (Mobility=50m/s)

No. of Malicious Nodes	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Throughput (kbps)					
2	16200	16536	16896	17930	18547	18953
4	15833	16350	16690	17330	18123	18716
6	15430	15798	16150	16759	17915	18230
8	14960	15166	15890	16161	17650	17850
10	14680	14936	15450	15793	16540	17115

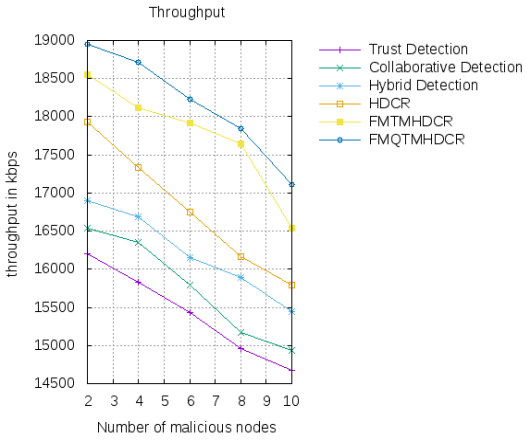

Fig. 1. Comparison of Throughput

Fig.1 shows that the throughput comparison of hybrid black/grayhole attack detection techniques for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes is taken in x-axis and the throughput values (Kbps) are taken in y-axis. It shows that the proposed FMQTMHDCR detection technique has better throughput compared with other techniques.

The comparison values of packet drop rate for existing and different proposed approaches are given in Table 3.

Table 3: Comparison of Packet Drop Rate (Mobility=50m/s)

No. of Malicious Nodes	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Packet Drop Rate (%)					
2	6.50	6.20	5.80	5.30	5.10	4.70
4	6.90	6.80	6.50	6.10	5.70	5.30
6	7.20	7.00	6.70	6.50	6.30	5.50
8	7.80	7.10	6.90	6.80	6.40	5.90
10	8.50	7.70	7.30	7.10	6.70	6.20

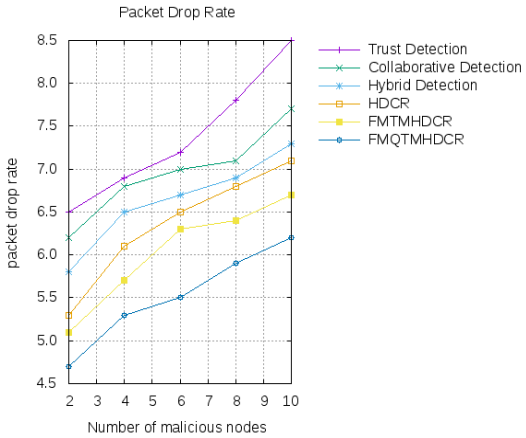

Fig. 2. Comparison of Packet Drop Rate

Fig. 2 illustrates that the packet drop rate comparison of hybrid black/grayhole attack detection techniques for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes is taken in x-axis and the packet drop rate values are taken in y-axis. It shows that the proposed FMQTMHDCR detection technique has reduced packet drop rate compared with other techniques.

The comparison values of packet delivery ratio for existing and different proposed approaches are given in Table 4.

Table 4: Comparison of Packet Delivery Ratio (Mobility=50m/s)

No. of Malicious Nodes	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Packet Delivery Ratio (%)					
2	69	73	77	82	85	92
4	65	70	75	80	81	87
6	62	67	71	76	80	83
8	59	63	68	73	78	81
10	56	61	65	71	76	79

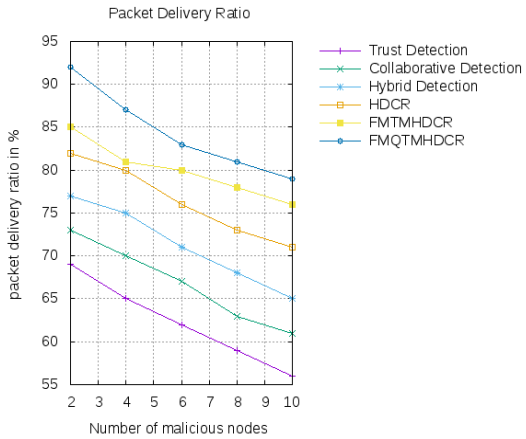

Fig.3. Comparison of Packet Delivery Ratio

Fig. 3 illustrates that the comparison of the packet delivery ratio for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes is taken in x-axis and in y-axis, the packet delivery ratio is taken. It proves that the proposed FMQTMHDCR detection technique has better packet delivery ratio compared with other techniques.

The comparison values of normalized routing overhead for existing and different proposed approaches are given in Table 5.

Table 5: Comparison of Normalized Routing Overhead (Mobility=50m/s)

No. of Malicious Nodes	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Normalized Routing Overhead					
2	0.17	0.14	0.12	0.09	0.06	0.04
4	0.23	0.20	0.15	0.12	0.09	0.08
6	0.27	0.22	0.19	0.15	0.13	0.10
8	0.31	0.28	0.24	0.21	0.18	0.15
10	0.38	0.31	0.27	0.23	0.19	0.17

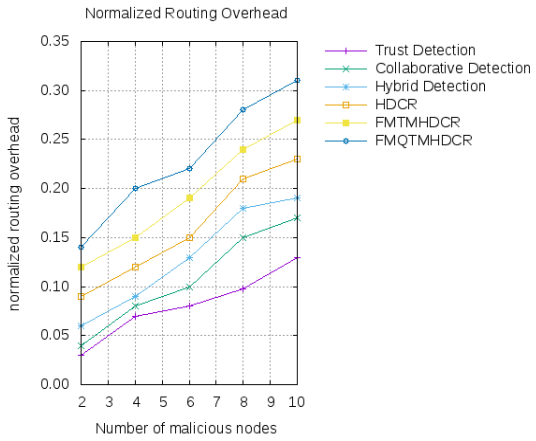

Fig. 4. Comparison of Normalized Routing Overhead

Fig. 4 illustrates that the normalized routing overhead comparison of hybrid black/grayhole attack detection techniques for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes is taken in x-axis and the normalized routing overhead values are taken in y-axis. It shows that the proposed FMQTMHDCR detection technique has better normalized routing overhead compared with other techniques.

C. Analysis of Fixed Number of Malicious Nodes with Varying Mobility of Nodes

The comparison values of throughput for existing and different proposed approaches are given in Table 6.

Table 6: Comparison of Throughput (No. of Malicious Nodes=10)

Speed (m/s)	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Throughput (kbps)					
5	16750	16936	17160	17453	17839	18150
10	16523	16670	16888	17251	17655	17962
15	16200	16350	16538	16984	17323	17539
20	16130	16290	16473	16756	17152	17213
25	15980	16075	16155	16435	16930	17047
30	15870	15996	16086	16167	16570	16950

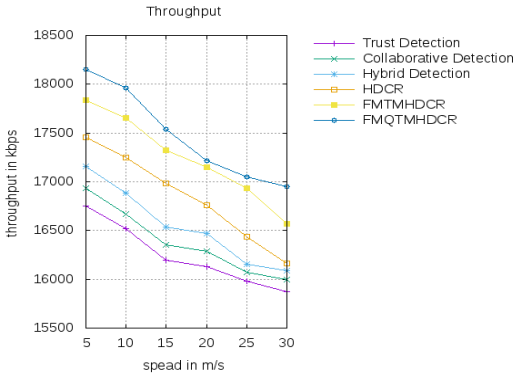

Fig. 5. Comparison of Throughput

Fig. 5 shows that the throughput comparison of hybrid black/grayhole attack detection techniques where the number of malicious nodes is 10. 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. It shows that the proposed FMQTMHDCR detection technique has better throughput compared with other techniques.

The comparison values of packet drop rate for existing and different proposed approaches are given in Table 7.

Table 7: Comparison of Packet Drop Rate (No. of Malicious Nodes=10)

Speed (m/s)	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Packet Drop Rate (%)					
5	7.20	6.90	6.50	6.00	5.80	5.40
10	7.30	7.10	6.80	6.40	6.10	5.60
15	7.70	7.30	7.00	6.80	6.50	5.80
20	7.90	7.40	7.20	7.10	6.70	6.20
25	8.30	8.10	7.60	7.40	7.00	6.50
30	8.60	8.20	7.90	7.50	7.20	6.90

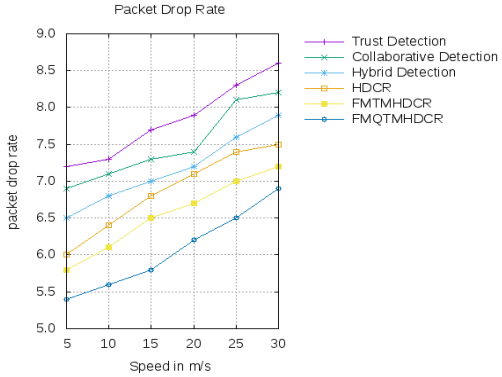

Fig. 6. Comparison of Packet Drop Rate

Retrieval Number: C4921098319/2019©BEIESP
DOI:10.35940/ijrte.C4921.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig. 6 shows that the packet drop rate comparison of hybrid black/grayhole attack detection techniques where the number of malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the packet drop rate values are taken in y-axis.

It shows that the proposed FMQTMHDCR detection technique has packet drop rate compared with other techniques.

The comparison values of packet delivery ratio for existing and different proposed approaches are given in Table 8.

Table 8: Comparison of Packet Delivery Ratio (No. of Malicious Nodes=10)

Speed (m/s)	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Packet Delivery Ratio (%)					
5	66	70	74	79	82	87
10	62	67	72	77	78	85
15	59	64	68	73	77	82
20	56	60	65	70	75	80
25	54	58	63	68	74	78
30	51	56	61	66	73	76

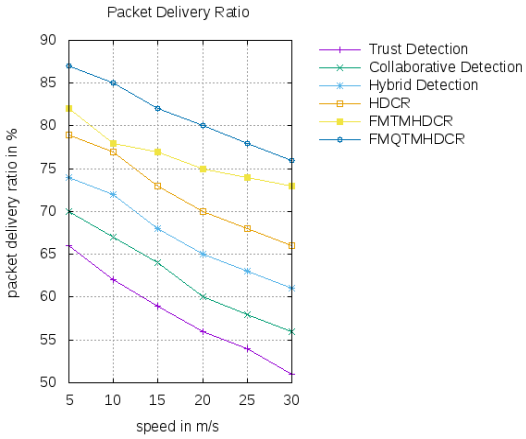

Fig.7 Comparison of Packet Delivery Ratio

Fig. 7 shows that the comparison of packet delivery ratio where the number of malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and in y-axis, the packet delivery ratio is taken. It proves that the proposed FMQTMHDCR detection technique has better packet delivery ratio compared with other techniques.

The comparison values of normalized routing overhead for existing and different proposed approaches are given in Table 9.

Table 9: Comparison of Normalized Routing Overhead (No. of Malicious Nodes=10)

No. of Malicious Nodes	Trust Detection	Collaborative Detection	Hybrid Detection	HDCR	FMTMHDCR	FMQTMHDCR
	Normalized Routing Overhead					
5	0.22	0.19	0.16	0.12	0.09	0.06
10	0.27	0.23	0.18	0.15	0.12	0.10
15	0.29	0.25	0.22	0.19	0.15	0.13
20	0.34	0.31	0.27	0.24	0.21	0.18
25	0.39	0.34	0.30	0.27	0.22	0.19
30	0.41	0.38	0.35	0.31	0.26	0.21

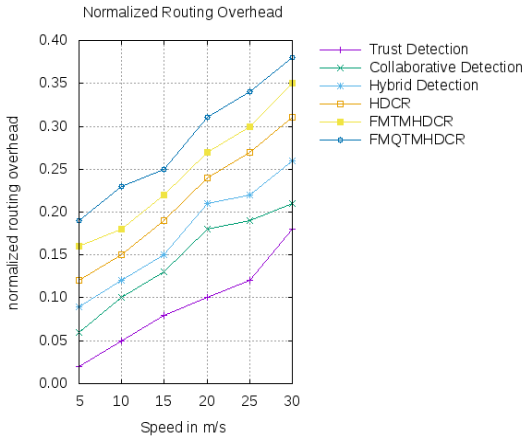

Fig. 8. Comparison of Normalized Routing Overhead

Fig. 8 shows that the normalized routing overhead comparison of hybrid black/grayhole attack detection techniques where the number of malicious nodes is 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. It shows that the proposed FMQTMHDCR detection technique has better normalized routing overhead compared with other techniques.

V. CONCLUSION

In this paper, the hybrid blackhole/grayhole attack detection technique is improved by considering the network metrics measurement such as DCR, mobility, traffic and queuing delay based on the fuzzy logic optimization technique. Initially, hybrid blackhole/grayhole attack detection technique is improved by measuring the DCR value for each node in the network to detect malicious node effectively. Moreover, the mobility and traffic measurement based hybrid detection technique is provided for selecting the routing path by removing the malicious node from routing table. Furthermore, the queuing delay is also measured in order to select the optimal routing path which is free from link failure as well as malicious node. Thus, the proposed FMQTMHDCR detection technique is effectively detect the malicious nodes in the routing path and remove the routing path with malicious nodes for transmitting data packets effectively without any attacks. The experimental results proved that the proposed FMQTMHDCR detection technique performs better than the other hybrid black/grayhole detection techniques.

REFERENCES

1. S. Singh, A. K. Pandey and M. Rani, "Generalized Black Hole Attack And Comparative Solution For MANET," Int. J. Emerg. Sci. Eng., vol. 1, no. 8, pp. 71-75, 2013.
2. A. Rana, V. Rana and S. Gupta, "EMAODV: Technique to Prevent Collaborative Attacks in MANETs," Procedia Comput. Sci., vol. 70, pp. 137-145, 2015.
3. G. S. Bindra, A. Kapoor, A. Narang and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," in IEEE Int. Conf. Syst. Eng. Technol., pp. 1-5, 2012.

4. J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," IEEE Syst. J., vol. 9, no. 1, pp. 65-75, 2015.
5. S. P. Dongare and R. S. Mangrulkar, "Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks," Procedia Comput. Sci., vol. 78, pp. 423-430, 2016.
6. V. A. Hiremani and M. M. Jadhao, "Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET," in IEEE Int. Conf. Green Comput. Commun. Conserv. Energy, pp. 944-948, 2013.
7. L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro and R. Magán-Carrión, "A model of data forwarding in MANETs for lightweight detection of malicious packet dropping," Comput. Netw., vol. 87, pp. 44-58, 2015.
8. A. Vangili and K. Thangadurai, "Detection of black hole attack in mobile ad-hoc networks using ant colony optimization–simulation analysis," Indian J. Sci. Technol., vol. 8, no. 13, 2015.
9. R. Vijayakumar and K. S. Kumar, "Detection of Black Hole Attack in Mobile AD-HOC Networks Using Hybrid Glow-worm Swarm Optimization (HGSO) Algorithm with Artificial Fish Swarm Algorithm (AFSA)," Int. J. Control Theory and Appl., vol. 9, no. 25, pp. 113-121, 2016.
10. G. Singh and N. Bhagat, "Removal of selective Black hole attack in Dynamic Source Routing (DSR) Protocol by alarm system," Int. J. Eng. Tech. Res., vol. 3, no. 6, pp. 129-131, 2015.
11. V. S. Subi and N. Nishanth, "Trust Assurance Mechanism against Gray Hole Attack in Mobile Ad Hoc Networks," Int. J. Adv. Trends Comput. Sci. Eng., vol. 4, pp. 01-05, 2015.
12. A. Haghighi, K. Mizanian and G. Mirjalily, "Improved MCBDS for Defending against Gray Hole and Black Hole Attacks in MANETs," Adv. Sci. Technol., vol. 10, no. 30, pp. 1-8, 2016.
13. K. Vijayakumar and K. Somasundaram, "An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet," Indian J. Sci. Technol., vol. 9, no. 36, 2016.
14. S. Makwana and K. Vaghela, "Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET," Int. J. Comput. Appl., vol. 125, no. 4, 2015.
15. S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in Proc. World Congr. Eng. Comput. Sci., pp. 22-24, 2008.
16. R. H. Jhaveri, S. J. Patel and D. C. Jinwala, "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks," in IEEE Second Int. Conf. Adv. Comput. Commun. Technol., pp. 556-560, 2012. IEEE.
17. P. Rathiga and S. Sathappan, "Hybrid detection of Black hole and gray hole attacks in MANET," in IEEE Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut., pp. 135-140, 2016.

AUTHORS PROFILE

Dr. P. Rathiga is working as Head of the Department in Navarasam Arts and Science College for Women, Department of Computer Applications, Arachalur, Erode, Tamil Nadu. She did Ph.D. from Bharathiar University, Coimbatore. Her area of research is Network Security and Wireless Network. She has a teaching experience of 13 years in Navarasam arts and Science College for women, Erode. She has guided 13 M.Phil. scholars. She has published 5 research papers in National and International Journals & presented 18 papers in National and International seminars and Conferences. She has delivered expert lectures on Cryptography and Network Security

Dr. S. Sathappan is working as Associate Professor in Erode arts and Science College (Autonomous), Department of Computer Science, Erode, Tamil Nadu. He did Ph.D from Bharathiar University, Coimbatore. His area of research is Digital Image Processing. He has a teaching experience of 33 years in Erode arts and Science College, Erode. He has guided 74 M.Phil. and 8 Ph.D. Scholars. He has published 45 research papers in various National and International Journals & presented 28 papers in National and International seminars and Conferences. He has delivered expert lectures on Digital Image Processing, Network Security and Data Mining. He is also a Syndicate Member of Bharathiar University from June 2015 to June 2018. He Served as a Senate Member of Bharathiar University, 2005-2008 and 2015-2018. He served as Board member of various Arts and Science colleges. He organized 12 National seminars and Conferences.He acts as a Recognized M.Phil guide for Bharathiar / Periyar / Manonmaniam /Alagappa / Bharathidasan / Annamalai / Mother Teresa Universities. He Published Study material books of School of Distance Education of Bharathiar University for B.Sc. Computer Science and PGDCA.