Hybrid and Secure Techniques for Simultaneous Detection of Black-Hole and Gray-Hole Attacks Using DSR Protocol in MANET

*Dr. P. Rathiga, #Dr. P. Sharmila

*Head, Department of computer Applications, #Principal, Navarasam Arts and Science College for Women, Arachalur, Tamil Nadu, India.

*rathiganavarasam@gmail.com, #dhyasharj@yahoo.co.in

Abstract - In MANET, the performance is degraded due to the black-hole and gray-hole attacks which cause the packet losses. In general, different detection and elimination approaches were developed for black-hole and gray-hole attacks separately [1]. But, the approaches for detecting both black-hole and gray-hole simultaneously are infrequent. Hence in this paper, a novel hybrid detection approach is proposed for detecting both black-hole and gray-hole attacks simultaneously in Dynamic Source Routing (DSR) protocol for MANET. In this hybrid approach, both black-hole and gray-hole attacks are detected based on the two detection threshold values. The performance evaluation of the proposed hybrid approach shows that it detects and eliminates the attacks effectively with better throughput, packet drop rate, packet delivery ratio and routing overhead.

Keywords: Black-hole and gray-hole attacks - Dynamic Source Routing protocol -Control packet ratio.

I. INTRODUCTION

Wireless network is a most widely used and important technology that allows users to access services and information electrically, regardless of its geographical position. And there are several types of networks available such as WMAN, WLAN, WWAN, WPAN, GAN, MANET, etc. MANET (Mobile Ad-hoc Network) is defined as the continuously self-configuring and infrastructure-less network of mobile nodes which are communicated wirelessly [2].

A. Attacks in MANET

Security of wireless network is one of a highly challenging issue. Understanding possible types of attacks are always very defective process of the entire network system. Some attacks acts against routing are listed as follows:

- Advertising the false route metric for misrepresenting the topology.
- Transmitting the route message with wrong sequence number for suppressing the other legitimate route messages.
- Flooding Route Discover excessively as a DoS attack.
- Modifying the Route Reply message for inserting the false route.
- Generating bogus Route Error for disrupting the working route.

In addition, attacks in MANET can be categorized into two types such as passive attacks and active attacks. The routing protocol is not disturbed by the passive attack. However this type of attack tries to find valuable information by listening to routing traffic and so the detection of these types of attacks has high complexity.

B. Black-hole Attack

In Black-hole routing attack, the fake routing information is transmitted to the other nodes from the malicious node claiming that it has an optimum path to destination and causes good nodes for routing the packets through the malicious nodes [8]. In AODV, the attacker can transmit the fake RREP with fake destination sequence number to the source node.

This causes the source node to select the path that passes through the malicious nodes so that all traffic will be routed through the malicious node. Therefore the malicious node can misuse or discard the traffic in MANET.

C. Gray-hole Attack

Gray-hole attack is also the misbehaviour of routing resulting communication failure. It involves two phases. One of the phases is node marketing which has the valid route to the destination node. In the second phase, the packets are intercepted by the nodes by using the specific match.

DOI : 10.35291/2454-9150.2019.0378

II. SURVEY

Vangili &Thangadurai *et al.* [3] proposed the Black-hole attack detection approach by using Ant Colony Optimization (ACO) in MANET. As such biology-inspired technique like ACO was utilized for modifying the AODV routing protocol. The ant which is located at each node was used for calculating its pheromone value by using the forwarding ratio at node. The proposed protocol was able to improve two main issues such as security and performance, but this approach was able to detect only one attack and effective for Black-hole.

Choudhury *et al.* [4] proposed Black-hole attack prevention method for implementing and improving the performance of AODV by Receive Reply method and presented modifications to the AODV protocol used in MANET. An algorithm was introduced for reducing the Black-hole attack on the routing protocols in MANET. The wait time and request reply tab table were generated to counter the Black-hole attacks and the AODV protocol. The proposed algorithm was simple and efficient with delay and congestion. But the method incorporated more time and computational complexity.

Chang *et al.* [5] described a cooperative bait detection approach 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 defence infrastructures. The reverse tracing technique was implemented by CBDS for achieving the objective of the proposed scheme. However, the security mechanisms were required for routing the packets.

Singh & Bhagat *et al.* [6] investigated the removal of selective Black-hole attack in Dynamic Source Routing (DSR) protocol. Here, the removal of Black-hole attack was described based on the alarm system used in the network by updating the malicious node detection in network and the packets were forwarded 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.

Kaur & Gupta *et al.* [7] proposed a novel technique for detecting and preventing the Black-hole attack in MANET. During this approach, a Meta heuristic search schema was introduced by integrating the min-max variants of ACO with Dynamic Route Pheromone bound value Information table (DRPI) based on the AODV routing protocol. This algorithm was proficient in providing an optimal path because operations to be performed in each node were very simple. Thus it was robust and fault tolerant. However, this protocol was not so efficient due to time limit.

A. *Survey analysis*

The previous researches related to Black-hole and Gray-hole attack detection and prevention schemes are discussed and analysed. After in this research, a novel hybrid black/Gray-hole detection approach is proposed for simultaneously detecting both the Black and Gray-hole attacks in DSR protocol for MANET by using the single approach. This Hybrid Detection system estimates the information distance metric based on the Kullback-Leibler distance for detection of Black-hole/Gray-hole attacks.

Then, two detection threshold values are assigned to identify both attacks in short time duration. By using the information about distance metric value of each node, the malicious or normal behavior of the node is determined by comparing with first detection threshold. The malicious nodes are compared with second detection threshold to determine whether the nodes perform Black-hole or Gray-hole attack. Thus, the Hybrid Detection approach detects the attacks better than most of the current techniques.

III. HYBRID BLACK/GRAY-HOLE ATTACK DETECTION APPROACH

In the proposed Hybrid Black/Gray-hole attack detection approach, initially the nodes are deployed in the DSR protocol for MANET . Then from the set of deployed nodes, the monitor nodes are initialized which collects the details about the packet flow of the neighboring nodes. When the source node forwards RREQ packets for the route discovery process as usual the attacker nodes replies RREP packets assigning itself high sequence number. The monitor nodes analyzing the packet flow of the neighboring nodes use the collected details to determine the information distance metric for all the nodes. Two detection thresholds are set and on comparing the information distance metric values of the nodes with the thresholds, the malicious nodes are detected [9].

Let N be the number of nodes deployed in the mobile ad-hoc networks. From the N number of deployed nodes, randomly choose some nodes as the monitor nodes to track the packet flow behavior of the deployed nodes. Using the information collected from the neighboring nodes A and B, the information distance metric value $D_\alpha(A, B)$ for each node is calculated. The information distance metric is computed as follows:

Two discrete complete probability distributions are considered i.e.

$$A = \{a_1, a_2, \dots, a_n\} \; and \; B = \{b_1, b_2, \dots, b_n\}$$

With $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i = 1, 1 \geq a_i \geq 0, 1 \geq b_i \geq 0, i = \{1,2, \dots, n\}$.

The information divergence is a measure of the divergence between P and Q and is given as follows:

$$D_\alpha(A||B) = \frac{1}{\alpha-1}\log_2\left(\sum_{i=1}^{n} a_i^\alpha b_i^{1-\alpha}\right), \alpha \geq 0 \qquad \text{……….} \; (1)$$

DOI : 10.35291/2454-9150.2019.0378

This information divergence of order is α and it is always non-negative if $\alpha \geq 0$. $D_\alpha(A||B) = 0$ Should be the minimum a distance and only if $A = B$. If A and B are incomplete probability distributions or $\alpha < 0$, then $D_\alpha(A||B)$ may be negative. The following special and useful formula is assumed based on the different α value, since α is an arbitrary positive parameter.

$$D_0(A||B) = -\log_2(\textstyle\sum_{i=1}^{n} b_i), \alpha = 0 \quad \ldots\ldots\ldots (2)$$

Moreover, the information distance is defined as follows:

$$D_\alpha(A,B) = D_\alpha(A||B) + D_\alpha(B||A)$$

$$= \frac{1}{\alpha-1}\log_2\left(\sum_{i=1}^{n} a_i^\alpha b_i^{1-\alpha} \times \sum_{i=1}^{n} b_i^\alpha a_i^{1-\alpha}\right) \quad \ldots\ldots\ldots (3)$$

Here, $D_\alpha(A,B)$ has a symmetric measure and always not less than $D_\alpha(A||B)$ and $D_\alpha(B||A)$. Thus, $D_\alpha(A,B)$ is measured as information distance metrics. Then, the two detection thresholds are set as σ_1 and σ_2. The first threshold σ_1 is for the detection of malicious nodes from the normal nodes while the second threshold σ_2 is for the determination or categorizing the malicious nodes into Black-hole and Gray-hole attackers separately. If the information distance metric value $D_\alpha(A,B)$ is greater thanσ_1, then the neighboring node is considered as malicious.

Simultaneously the second threshold σ_2 is also compared. If $D_\alpha(A,B)$ is less than σ_2 but greater than σ_1, the node is Gray-hole attacker while $D_\alpha(A,B)$ is greater than σ_2, the node is marked as Black-hole attacker. If these conditions are not satisfied the node is considered as normal node. When the nodes are detected as malicious (Black/Gray-hole) the monitor node updates it in the malicious list M and advertises the node details to the whole network. The nodes that remain in the network update the routing table using the advertised messages.

IV. PERFORMANCE EVALUATION

In this section, the performance of the proposed collaborative black/Gray-hole attack detection mechanism and hybrid Black/Gray-hole attack detection approach in the DSR protocol for MANET are evaluated and compared with Trust-based Black-hole attack detection method [10]. Generally, MANET utilizes the simulation research tool named as Network Simulator version 2.34 (NS-2.34) which is the discrete event simulator.

Performance Metrics

A. Throughput

$$Throughput = \frac{Numberoftransmittedpackets}{Timetaken}$$

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

B. Packet Drop Rate

$$PacketDropRate = \frac{Numberofdroppedpacketsatdestination}{Totalnumberofpacketsgeneratedatsource}$$

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.

C. Packet Delivery Ratio

$$PacketDeliveryRatio = \frac{Total\ numberofpacketsreceivedbydestination}{Totalnumberofpacketssentbysource}$$

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.

D. Normalized Routing Overhead

$$RoutingOverhead = \frac{Totalnumberofroutingpacketstransmitted}{Totalnumberofdatapacketsreceived}$$

The fraction of the amount of routing packets like RREQ and RREP forwarded per data packet is known as Normalized Routing Overhead.

The performance metrics are evaluated for two types of simulation scenario such as

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

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

3.4.2 Varying the Number of Malicious Nodes with Fixed Mobility.

In this Scenario 1, the speed of the node is 50 m/s and the number of malicious nodes are 2, 4, 6, 8 and 10. Then the performance matrices such as Throughput, Packet Delivery Ratio, Packet Drop Rate and Normalized Routing Overhead are compared under this Scenario.

Throughput

Table 4.1 shows the experimental results of Throughput with respect to different number of malicious nodes. The existing methods such as Trust Detection and Collaborative Detection are compared with the proposed Hybrid Detection technique in terms of Throughput. If Throughput value is high, than the technique is considered as more efficient. From the Table, it is clear that the proposed

DOI : 10.35291/2454-9150.2019.0378

Hybrid Detection technique improves the Throughput than other existing methods.

Table 4.1 Performance Comparison of Hybrid Detection Scheme in terms of Throughput under Scenario 1

No. of Malicious Nodes	Throughput (Kbps)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
2	14860	16200	16536	16896
4	13350	15833	16350	16690
6	12962	15430	15798	16150
8	12030	14960	15166	15890
10	11875	14680	14936	15450

Packet Drop Rate

The comparative study of proposed Hybrid Detection technique with existing methods such as Trust Detection and Collaborative Detection in terms of Packet Drop Rate is observed and simulation results are given in Table 4.2. The number of malicious nodes with speed 50 m/s is taken as input for performing the experiments.

The proposed Hybrid Detection technique is compared with existing methods in terms of Packet Drop Rate. From the Table 3.3, it is observed that three methods significantly reduce the Packet Drop Rate for secured path selection on the different number of malicious nodes. But comparatively, the proposed Hybrid Detection technique minimizes the Packet Drop Rate than other existing methods.

Table 4.2 Performance Comparison of Hybrid Detection Scheme in terms of Packet Drop Rate under Scenario 1

No. of Malicious Nodes	Packet Drop Rate (%)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
2	7.10	6.50	6.20	5.80
4	7.80	6.90	6.80	6.50
6	8.50	7.20	7.00	6.70
8	9.10	7.80	7.10	6.90
10	9.80	8.50	7.70	7.30

Packet Delivery Ratio

Table 4.3 has the experimental results of Packet Delivery Ratio with respect to the number of malicious nodes. The malicious nodes varied from 2 to 10 with the speed of node is 50 m/s which is taken as input for performing the experiment. In order to carry out the simulation, the proposed Hybrid Detection technique is compared with existing methods. From the Table, it is observed that three methods significantly increase the Packet Delivery Ratio based on the number of malicious nodes. But, comparatively the proposed technique gives better results than other existing methods.

Table 4.3 Performance Comparison of Hybrid Detection Scheme in terms of Packet Delivery Ratio under Scenario 1

No. of Malicious Nodes	Packet Delivery Ratio (%)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
2	60	69	73	77
4	54	65	70	75
6	49	62	67	71
8	42	59	63	68
10	37	56	61	65

Normalized Routing Overhead

The performance of Normalized Routing Overhead using proposed Hybrid Detection technique with existing Trust Detection and Collaborative Detection are shown in Table 4.4. The number of malicious nodes taken from the range of 2 to 10 which moves at fixed mobility of 50 m/s is considered as input to carry out the simulation. It is clear that Normalized Routing Overhead Significantly reduced in the Hybrid Detection technique when compared to the existing methods. For example when the number of malicious node is 10, the Normalized Routing Overhead value for Hybrid Detection technique is 0.27 which is less than the values of Trust Detection and Collaborative Detection methods.

Table 4.4 Performance Comparison of Hybrid Detection Scheme in terms of Normalized Routing Overhead under Scenario 1

No. of Malicious Nodes	Routing Overhead Range (0 to 1)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
2	0.19	0.17	0.14	0.12
4	0.26	0.23	0.20	0.15
6	0.29	0.27	0.22	0.19
8	0.33	0.31	0.28	0.24
10	0.41	0.38	0.31	0.27

3.4.3 Varying the Mobility of Nodes with Fixed Number of Malicious Nodes

Scenario 2 denotes that the malicious nodes are fixed as 10 and the mobility of the nodes varied from 5 m/sec to 30 m/sec. Then the performance matrices such as Throughput, Packet Delivery Ratio, Packet Drop Rate and Normalized Routing Overhead are evaluated under this Scenario.

Throughput

Table 4.5 describes the experimental results of Throughput with respect to various speed of malicious node.

Table 4.5 Performance Comparison of Hybrid Detection Scheme in terms of Throughput under Scenario 2

Speed (m/sec)	Throughput (Kbps)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
5	16432	16750	16936	17160
10	16100	16523	16670	16888
15	15986	16200	16350	16538
20	15630	16130	16290	16473
25	15126	15980	16075	16155
30	14910	15870	15996	16086

The proposed Hybrid Detection technique is compared with existing methods such as Trust Detection and Collaborative Detection in terms of Throughput and it is observed that the proposed Hybrid Detection technique increases the Throughput than the other two existing methods. For example, Throughput of proposed Hybrid Detection is 17160 kbps when speed of mobility is 5 m/sec whereas Collaborative Detection is 16936 kbps and Trust Detection is 16750 kbps.

Packet Drop Rate

The Packet Drop Rate comparison of the proposed technique with the existing techniques is shown in Table 4.6. It is observed from the table that the Proposed Hybrid Detection technique provides better results in terms of Packet Drop Rate. When considering the mobility speed as 30, Packet Drop Rate value obtained for the proposed Hybrid Detection technique is 7.90 whereas Packet Drop Rate value obtained for existing Trust Detection and Collaborative Detection are 8.60 and 8.20 respectively.

Table 4.6 Performance Comparison of Hybrid Detection Scheme in terms of Packet Drop Rate under Scenario 2

Speed (m/sec)	Packet Drop Rate (%)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
5	7.80	7.20	6.90	6.50
10	8.00	7.30	7.10	6.80
15	8.30	7.70	7.30	7.00
20	8.70	7.90	7.40	7.20
25	9.00	8.30	8.10	7.60
30	9.40	8.60	8.20	7.90

Packet Delivery Ratio

Table 4.7 presents the measurement of Packet Delivery Ratio by using proposed Hybrid Detection technique, existing Trust Detection and Collaborative Detection. It is observed from Table 3.8, Packet Delivery Ratio value obtained for the proposed technique is 63% when the mobility speed is 25 whereas the Packet Delivery Ratio value obtained for the existing Trust Detection and Collaborative Detection techniques are 54% and 58% respectively. Thus, the above results confirm that the proposed technique produces better results than all the existing techniques.

Table 4.7 Performance Comparison of Hybrid Detection Scheme in terms of Packet Delivery Ratio under Scenario 2

Speed (m/sec)	Packet Delivery Ratio (%)			
	Network Without Attack Detection	Trust Detectio n	Collaborati ve Detection	Hybrid Detection
5	60	66	70	74
10	54	62	67	72
15	49	59	64	68
20	42	56	60	65
25	38	54	58	63
30	34	51	56	61

Normalized Routing Overhead

Table 4.8 gives the performance of Normalized Routing Overhead using proposed Hybrid Detection technique with the existing methods. It conveys that the Normalized Routing Overhead is decreased for different speed of malicious nodes. For example, the Normalized Routing

DOI : 10.35291/2454-9150.2019.0378

Overhead for the proposed method is 0.30 when the speed of malicious node is 25 m/sec whereas existing Trust Detection and Collaborative Detection are 0.39 and 0.34 respectively. But comparatively Normalized Routing Overhead attains better results in the proposed Hybrid Detection technique when compared to the existing mechanism.

Table 4.8 Performance Comparison of Hybrid Detection Scheme in terms of Normalized Routing Overhead under Scenario 2

Speed (m/sec)	Routing Overhead Range (0 to 1)			
	Network Without Attack Detection	Trust Detection	Collaborative Detection	Hybrid Detection
5	0.25	0.22	0.19	0.16
10	0.30	0.27	0.23	0.18
15	0.31	0.29	0.25	0.22
20	0.36	0.34	0.31	0.27
25	0.42	0.39	0.34	0.30
30	0.43	0.41	0.38	0.35

V. CONCLUSION

In this paper, the hybrid Black/Gray-hole attack detection approach is proposed to tackle both the attacks using the same algorithm in DSR protocol. The hybrid approach initializes monitor nodes for the collection of Packet flow information from the neighboring nodes. Then using the collected information, the information distance metric is calculated for all the nodes. Two detection thresholds are set for detecting both black and Gray-hole attacks in a single step. If the information distance metric value of a node is greater than both the thresholds, the node is considered as Black-hole attacker and if the value is above first threshold while below the second threshold, the node is considered as Gray-hole attacker.

Thus both the attacks are detected in a single process. Experimental results show that the proposed Hybrid Detection approach performs better than the other Black/Gray-hole attack detection mechanisms.The analysis results show that the degree of impact for attacks depends on the parameters used. The impact of attacks increases significantly with an increasing number of malicious nodes and node mobility. Also, this analysis is used for estimating the damage caused by these attacks and determining adequate counter measures. Moreover, it is concluded that Throughput and Packet Delivery Ratio are reduced due to the attacks in the network whereas these increased when attacks are detected and prevented. Similarly, Packet Drop Rate and Normalized Routing Overhead increased due to the attacks, but both reduced during detecting and preventing the attacks within the network.

REFERENCES

[1] Singh, S., Pandey, A. K., & Rani, M. Generalized Black-hole attack and comparative solution for MANET. *International Journal of Emerging Science and Engineering (IJESE)*, *1*(8) 71-75, June, 2013.

[2] Nasir, H. J. A., & Ku-Mahamud, K. R. Wireless Sensor Network: A Bibliographical Survey. *Indian Journal of Science and Technology*, *9*(38), 2016.

[3] Vangili, A., &Thangadurai, K. Detection of Black-hole attack in mobile ad-hoc networks using ant colony optimization–simulation analysis. *Indian Journal of Science and Technology*, *8*(13), 2015.

[4] Choudhury, D. R., Ragha, L., &Marathe, N. Implementing and improving the performance of AODV by receive reply method and securing it from Black-hole attack. *Procedia Computer Science*, *45*, 564-570, 2015.

[5] Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE systems journal*, *9*(1), 65-75, 2015.

[6] Singh, G., &Bhagat, N. Removal of selective Black-hole attack in Dynamic Source Routing (DSR) Protocol by alarm system. *International Journal of Engineering and Technical Research (IJETR)*, *3*(6), 129-131, 2015.

[7] Kaur, S., & Gupta, A. A Novel Technique to Detect and Prevent Black-hole Attack in MANET. *International Journal of Innovative Research in Science, Engineering and Technology*, *4*(6), 4261-4267, 2015.

[8] Jamali, S. B. S. A survey over Black-hole attack detection in mobile ad hoc network. *International Journal of Computer Science and Network Security (IJCSNS)*, *15*(3), 44-51, 2015.

[9] Rathiga, P. & Sathappan S. Hybrid detection of Black hole and gray hole attacks in MANET. International conference on *Computation System and Information Technology for Sustainable Solutions (CSITSS)*, (pp. 135-140) IEEE Xplore. INSPEC Accession Number: 16525753. DOI: 10.1109/CSITSS.2016.7779411.

[10] Thachil, F., &Shet, K. C. A trust based approach for AODV protocol to mitigate Black-hole attack in MANET. In *Computing Sciences (ICCS), 2012 International Conference on* (pp. 281-285). IEEE, September, 2012.

DOI : 10.35291/2454-9150.2019.0378