Black Hole Attack Detection In Mobile Ad Hoc Networks Using Optimization Techniques

Dr. R.Sujatha

Assistant Professor & Head, Department of Computer Science, Queens College of Arts and Science for Women (Affiliated to Bharathidasan University, Tiruchirappalli), Punalkulam, Pudukkottai.

ABSTRACT

A mobile ad-hoc network (MANET) is a wireless mobile node network that is generated on the fly. In a MANET, it is assumed that all nodes can work together to transmit data packets in a multi-hop manner. Some malicious nodes, on the other hand, refuse to cooperate with other nodes and cause network disruption by providing false routing information. Any node in a MANET can join or leave the network at any time. Using given routing protocols and mobility models, nodes may send and receive data. MANETs are vulnerable to various network layer attacks due to the lack of a centralised infrastructure. Network layer attacks such as Worm Hole, Black Hole, Gray Hole, Byzantine, and Sybil Attacks disrupt network topology, resulting in data loss and network degradation. A node declares itself to have the nearest paths to all of the destinations in the Black Hole Attack. Through using the routing protocol, this node consumes all of the network's data packets, lowering network performance. In this study, optimization algorithms are used to locate the MANET's black hole node. To find the single black hole attack in the network, the optimization algorithms Artificial Bee Colony (ABC) and Particle Swarm Optimization (PSO) are combined. The performance of the proposed Optimizations based on Single Black Hole Attack (OSBHA).

KEYWORDS: Mobile Ad Hoc Network (MANET), Denial of Service Attacks, Black Hole Attack, Optimization Algorithm, Malicious Node

1. INTRODUCTION

Due to the current proliferation of cutting-edge technology, mobile ad-hoc networks (MANETs) have gained a major reputation in recent years (i.e., smartphones, tablets, personal digital assistants, etc.) 1st. Nodes are wirelessly linked to each other to pass data packets due to the dynamic world. Since data packets are transported between nodes over an open medium with no central support, nodes can exchange information at any time in the network. If the source and destination nodes are not in the same range, the communication's reliability is solely dependent on the intermediate nodes' ability to reliably forward data packets. If it is close to the source node, an intermediate node acts as a host and communicates directly with it, while if it is far away from the destination node, it acts as a router [2]. Wireless nodes, on the other hand, have limited resources, such as low battery capacity, limited memory, and limited bandwidth. The MANET was created with the aim of allowing nodes to communicate quickly and easily. It's used on battlefields, in emergency relief, rescue operations, maritime communications, personal or commercial data sharing, and in places where wired connectivity isn't available. The implementation of the MANET does not necessitate any special infrastructure, and it is inexpensive to set up anywhere [3] [4]. When a source node needs to send data packets over an open medium to a specific node, it uses multi-hop with the aid of intermediate nodes. Any malicious nodes can easily access the network due to the dynamic topology, unstructured network, open medium, and high mobility of the nodes. Malicious nodes attempt to disrupt network resources by dropping data packets, stealing important information, or manipulating data packets, resulting in undesirable outcomes, a phenomenon known as a Denial of Service (DoS) attack [5].

2. BACKGROUND STUDY ON BLACK HOLE ATTACK

A Denial-of-Service (DoS) attack is any event that reduces or removes a network's ability to perform its intended purpose. The aim is to deny network services to nodes, resulting in data packets being dropped and network bandwidth being reduced by preventing approved users from accessing resources [6]. The taxonomy of DoS attacks is depicted in Figure 1. DoS attacks in MANETs are classified into two types: absolute packet drop attacks (black hole attacks) and partial packet drop attacks (gray hole attacks) [7]. Black hole attacks can be divided into three categories: single hole attacks, multiple attacks, and collective attacks. A single node or a group of nodes may engage in malicious activity, as their names suggest. A gray hole attack, on the other hand, is a partial packet drop attack. It can also be divided into two types of attacks: sequence-based and smart gray hole attacks.

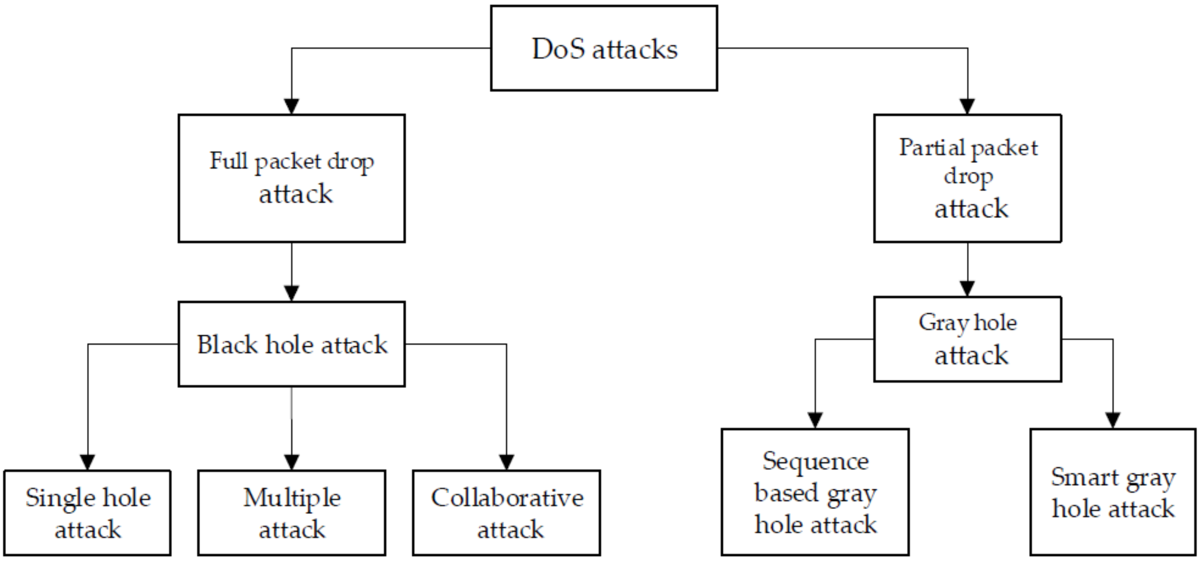

Figure 1: Classification of Denial of Service (DoS) Attacks

2.1 Black Hole Attacks

A black hole attack is a form of Denial of Service (DoS) attack that is one of the protuberant attacks. In MANETs, it's also known as a complete packet drop attack. Because of the open medium and complex topology of MANETs, a black hole node can easily and stealthily join the network. During the route discovery process, black hole nodes become visible. Initially, there is no valid route from the source node to the destination node. For route discovery, the source node sends a route request (RREQ) packet to the intermediate nodes. When a valid node receives an RREQ packet from a source node, it forwards it to the next node if it is not a destination node; however, when a black hole node receives an RREQ, it sends a bogus route reply (RREP) with a high sequence number to win the route search. The sequence number is used to determine the route's freshness, or how often it is changed. The black hole node deceives the source node into believing it has a true, short, and fresh route to the destination node, despite the fact that it does not. In this way, the black hole node sends a signal to the source node and becomes involved in the network's path between the starting node (source node) and the final node (destination node). After the route has been defined, the source node begins sending data packets to the black hole node, which eventually drops all data packets without forwarding them to the destination node [8][9][10][21][22][23][24][25][26].

3. RELATED WORKS

Sivanesh, S., and VR Sarma Dhulipala [11] For detecting the most vulnerable packet dropping attack known as a black hole attack, researchers created the ‘Accurate and Cognitive Intrusion Detection Method' (ACIDS). This method considers parameters such as Destination Sequence Number (DSN) and Route Reply (RREP) when detecting intruders by recognising deviations from standard behaviour of the chosen parameters.

Elmahdi, Elbasher, Seong-Moo Yoo, and Kumar Sharshembiev [12] based on modified ad-hoc on-demand multipath distance vector (AOMDV) protocol, proposed a new approach to provide reliable and stable data transmission in MANETs under potential blackhole attacks. We split the message into several paths to the destination and encrypt it with a homomorphic encryption scheme. The proposed scheme's performance is stable even with a high packet delivery ratio, while AOMDV's performance is found to be vulnerable when malicious nodes are introduced into the network.

Rameshkumar, S. G., and G. Mohan [13] proposed a modified Ad-hoc on-demand Distance Vector (AODV) with timeout duration analysis for each transmitted packet from the nodes, as well as queuing analysis, to compute the average, minimum, and maximum packet transmission delays. The original AODV protocol was updated to use timeout duration analysis to identify malicious nodes that should be converted to single or cooperative black hole nodes, and then delete them from the network.

Cherkaoui, Badreddine, Abderrahim Beni-hssane, and Mohammed Erritali [14] proposed a novel method for detecting such an attack in a VANET network during contact. This approach is based on a variable control map, which is commonly used in industry to measure the output of a process. By installing the monitoring device in each receiving node within the network, this approach will detect malicious nodes in real time.

Kumar, Ankit, et al [15] For detecting black hole attacks, a reliable AODV routing protocol was developed. The proposed method is a modified version of the original AODV routing protocol, with improved RREQ and RREP packet protocols. For added security, a cryptography function-based encryption and decryption is included to verify the source and destination nodes.

Aranganathan, A., C. D. Suriyakala, and V. Vedanarayanan [16] When compared to existing routing protocols, the proposed Software Agents-based Black Hole attacks Detection and Prevention in Clustering Ad hoc On-Demand Distance Vector (SABHDP-CAODV) routing protocol is based on the unique identity of legitimate nodes, location-based distance calculation, threshold time, simulation metrics of packet delivery ratio throughput, average end-to-end delay, and network routing overhead.

Bhardwaj, Suyash, and Vivek Kumar [17] exhibited In AODV, we use a Secure Cooperative Neighbour-Based Approach to detect and avoid black hole attacks right from the outset. This method allows each node to communicate with its neighbour in a safe, reliable, and fast manner while also protecting against routing attacks by taking a different path when locating an intruder.

Gayathri, V. M., and P. Supraja [18] Concerned about a network black hole attack that causes packets to be dropped that were supposed to be sent to the destination. The comparative results of different performance factors based on the scenario used are also included in this article. That is, it contrasts the effects of intruder nodes with and without them. Regression Based Intruder Detections (RBIDS) is an algorithm proposed to improve network efficiency by detecting malicious nodes. This algorithm is used to measure the output of each individual node over a period of time using regression values.

Khan, Dost Muhammad, et al [19] The use of Ant Colony Optimization Technique and Repetitive Route Configuration with Reactive Routing Protocol to prevent Black Hole Attacks in mobile ad-hoc networks was discussed. This study found that using ACO with Reactive Routing Protocol resulted in higher useful throughput and better protection of Black Hole Attacks, with a 10% increase in throughput and a 27% reduction in packet loss over Least Cost Path Protocol.

Ponnusamy, Muruganantham [20] In a Mobile Ad-hoc Network, nodes that are located in an open environment and travel randomly from one location to another are vulnerable to security threats. As a result, in MANET, the node credibility and energy efficient model is used to reduce the annoyance caused by selfish nodes and to delete them from the system during routing operations. The network's reputable and energy-efficient nodes are marked, and data transmission follows safe paths. The malicious nodes, on the other hand, are not cooperating with each other in this reputation scheme. The reputed nodes are identified by examining the contact ratio between them.

4. PROPOSED OPTIMIZATION BASED SINGLE BLACK HOLE DETECTION IN MANET

A successful metaheuristic algorithm combines exploitation of prior information gathered at some point during the search process with exploration of new areas in the search space, which can lead to more optimal results. Particle Swarm Optimization (PSO) is an optimizer based on the social behaviour of flocking birds and schooling fish. It appears to have a strong ability to efficiently explore and exploit the search space by using a variety of factors that affect exploitation versus exploration. The equations used to change the swarm's current location, best previous position, and flying velocity are as follows. Each node (particle I track three values directly in the procedure: its current location (X_i), the optimum route position it arrived in previous cycles (P_i), and its flying velocity (V_i).

$$Present\ Position\ X_i = (x_{i1}, x_{i2}, \dots, x_{is}) \qquad (1)$$

$$Finest\ Previous\ Position\ P_i = (p_{i1}, p_{i2}, \dots, p_{is}) \qquad (2)$$

$$Flying\ Velocity\ V_i = (v_{i1}, v_{i2}, \dots, v_{is}) \qquad (3)$$

The location (position) (P_g) denotes the global optimal route path on the entire MANET for each time interval (cycle). As a result, every node (particle) improves its velocity V_i in order to get closer to the best route path g, as shown below:

$$New\ V_i = \omega + current\ V_i + c_1 \times rand() \times (P_i - X_i) + c_2 \times Rand() \times (P_i - X_i) \quad (4)$$

As a result, the particle's productive location when using the novel velocity V_i is:

$$Newposition\ X_i = Currentposition\ X_i + New\ V_i\ V_{max} \geq V_i \geq -V_{max} \qquad (5)$$

Where $c_1 = c_2 = 2$ → two positive constants provide learning parameters, rand() and Rand() indicate two random purposes in the ranges [0,1], V_{max} represents the upper limit on the maximum change of particle velocity, gives inertia weight engaged as an improvement to direct the authority of the previous history of velocities on the current velocity, and it provides local and global search, and it is initiated to diminish linearly with time from a worth of 1.4 – 0.5.

On the other hand, the ABC is better at locating local optima thanks to the two phases of employee and onlooker, both of which are called local search operators. The onlooker bees fly straight to one of the working bees' better nectar sources. ABC is primarily concerned with identifying strategies that enhance local search. The key difference between working bees and onlooker bees is that the latter selects a solution based on the likelihood of it having a high fitness benefit. Furthermore, the scout step of the ABC algorithm implements global search, resulting in a slower convergence speed during the search process.

Algorithm: Optimization based Black Hole Attack (OBHA) Detection

```
Input: Objective function f(x), and constraints.
Step 1: Parameter Initialization: MG (Maximum Number of Generation); FS (Number of Food Source); Limit; Swarm social and cognitive components; rand () and Rand (); inertia; $V_{max}$.
Step 2: Initialization of Population: The swarm's population $a_i = (i = 1,2, \dots, FS)$, step vector $\Delta a_i = (i = 1,2, \dots, FS)$;
Step 3: Set Prob = 0.1 and Generation iteration = 0;
Step 4: Starting Iterations (it)
    Step 4.1: While it ≤ MG do
        Step 4.1.1: for i = 1, 2, …, FN
            Step 4.1.1.1: if $rand \leq Prob$ then
                1. Begin of PSO
        2. Calculate the number of nodes in networks as initial population of N solutions(particles);
        3. For each node $i \in$ N; Calculate the Fitness (i) depending on DRI table.
        4. Consider the weight factor and inertia.
        5. For each node;
          Set $p_{Best}$ as the best route position of nodes (particle) i;
                6. If fitness (i) is better than $p_{Best}$ in the current route.
                7. $p_{Best(i)} = fitness\ (i)$
                8. End;
                9. Set $g_{Best}$ as the best fitness of all particles (nodes)
                10. If a particle $p_{Best} > g_{Best}$
                    Update velocity of that particle using equation (4)
                    Update position of that particle using equation (5)
                11. Else
                    Update the value of the weight, and inertia.
                12. End if
                13. Evaluate the fitness value of each candidate solution
                14. Apply a greedy selection process to select the best one;
        15. If a solution does not improve, traili =traili+1, otherwise traili=0
        16. Check and correct the new positions based on the boundaries of variables.
        17. End Process of PSO.
      Step 4.1.1.2: else
        1. Input: A particle position $x_i$
        2. Select high fitness values from all $x_i$.
        3. Calculate the probability values p for the selected $x_i$ using $Pr_i = \left(\frac{fit_i}{\sum_{i=1}^{FS} fit_i}\right)$
        4. For each of particle bee do
            If $rand\ (0,1) \leq P$ then
                Update a new produced solution $x_i$ by using
                $fit_i = 1 + c_1 c_2 \omega(fit_i)\ or\ \left(\frac{1}{1} + fit_i\right)$
                $x_{ij} = x_{ij} + \emptyset_{ij}(x_{ij} - x_{kj})$
            Apply a greedy selection process to select the best solution.
            End if
                5. End for
                6. Output: the new position $x_i$
            Step 4.1.1.3: end if (Scout Bee Modification Phase)
                1. Input: A particle bee position $x_i$
                2. Update a new produced solution $x_i$ using equation (6)
                3. Apply a greedy selection process to select the best solution.
                4. Output: the new position $x_i$
        Step 4.1.2: end for
    Step 4.2: end while
Step 5: The best node (Genuine Node)
```

The key contribution of optimization-based single black hole attack detection is based on two major improvements: first, modifying the scout bee process in the ABC algorithm to increase search diversity and counterbalance the shortfall in global search efficiency of the ABC algorithm. The second enhancement is to incorporate PSO operators from PSO into ABC as a substitute for the regular ABC's first step (employee bee phase). The Scout bee modification process plays a similar role in the proposed algorithm as it did in the original ABC algorithm. The proposed algorithm will search to see if there are any exhausted sources that should be abandoned after both the particle-bee and onlooker bee phases are completed. To determine if the source should be abandoned, special counters are used. When a particle-bee is unable to bring better new solutions in the previous processes, these counters are incremented. The food source is replaced with a new source if the counter value exceeds the parameter limit, and the resulting particle-bee becomes a new scout bee. Using the following equation (6), the updated scout bee generates a new food source to replace s_i, assuming the abandoned source is s_i:

$$s_i^{t+1} = 0.5 \times rand \times \left(s_i^t - -best\ solution\right) \qquad (6)$$

Only one source can be exhausted in each loop, and only one particle-bee can be a scout, according to the proposed algorithm. If more than one counter exceeds the limit value, the programme can choose one of the maximum counters. In the original ABC, the scout bee process produces the solution at random, which adds variety to the quest. However, as a result of the iterations, the convergence rate will be reduced. The proposed algorithm's updated scout bee step preserves search diversity by selecting a new food source at random, resulting in good exploration, but it also leads to exploitation by considering the best solution so far and producing a new solution based on both the current and best solutions, as shown in Equation (6).

5. RESULT AND DISCUSSION

5.1 Simulation Parameters

The following table 1 depicts the simulation parameters used in this research work.

Table 1: Simulation Parameters

Parameters	Values
Routing protocol	Ad-hoc On-Demand Distance Vector
Transmitter range	300m
Simulation time	200s
Bandwidth	2 Mbits/s
Scenario size	1000 9 1000 m^2
Number of nodes	80
Packet size	64 bytes
Traffic type	Constant Bit Rate
Rate	4 packets/s
Simulator	NS2

The evaluation metrics like Packet Delivery Ratio (PDR), Detection Rate, Routing Overhead, Throughput, and Average end-to-end delay are considered in this research work to evaluate the performance of the proposed methodology for finding the single black hole in the network. The performance of the proposed Optimization based Black Hole Attack (OBHA) Detection is analysed with PSO based AODV, and ABC based AODV protocols.

Table 2 depicts the Packet Delivery Ratio (PDR) obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes. From the table 2, it is clear that the proposed OBHA detection method gives more PDR when it is compared with other optimization techniques based AODV protocol.

Table 2: Packet Delivery Ratio (PDR) obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes

Number of Nodes	Packet Delivery Ratio (PDR) by AODV protocols		
	Proposed OBHA	PSO	ABC
10	92.63	84.34	85.81
20	92.81	84.73	86.20
30	93.27	85.14	86.57
40	93.74	85.88	87.14
50	94.31	86.24	87.96
60	94.82	86.55	88.22
70	95.21	87.17	88.63
80	95.78	87.86	89.12

Table 3 depicts the Detection Rate (DR) obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes. From the table 3, it is clear that the proposed OBHA detection method gives more detection rate when it is compared with other optimization techniques based AODV protocol.

Table 3: Detection Rate obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes

Number of Nodes	Detection Rate by AODV protocols		
	Proposed OBHA	PSO	ABC
10	93.14	85.45	86.43
20	93.92	86.95	87.38
30	94.69	85.73	87.95
40	94.93	86.79	88.26
50	95.52	87.45	89.17
60	95.97	87.92	89.64
70	96.52	88.36	89.81
80	96.89	88.84	90.24

Table 4 depicts the Routing Overhead obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes. From the table 4, it is clear that the proposed OBHA detection method reduced the routing overhead when it is compared with other optimization techniques based AODV protocol.

Table 4: Routing Overhead obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes

Number of Nodes	Routing Overhead (in bytes) by AODV protocols		
	Proposed OBHA	PSO	ABC
10	3014	3576	3312
20	3373	3693	3427
30	3499	4125	4238
40	3658	4439	4529
50	4189	4817	4711
60	4357	5358	5289
70	4745	5947	5817
80	5264	6556	6429

Table 5 depicts the Throughput obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes. From the table 5, it is clear that the proposed OBHA detection method gives more throughput when it is compared with other optimization techniques based AODV protocol.

Table 5: Throughput (Kbps) obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes

Number of Nodes	Throughput (Kbps) by AODV protocols		
	Proposed OBHA	PSO	ABC
10	68.17	58.42	64.181
20	69.49	60.64	66.26
30	71.57	62.82	67.51
40	72.78	63.74	68.43
50	73.56	64.38	69.52
60	75.78	65.59	70.77
70	78.96	66.47	71.96
80	79.81	68.56	72.885

Table 6 depicts the Average End-to-End delay obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes. From the table 6, it is clear that the proposed OBHA detection method reduced End-to-End delay when it is compared with other optimization techniques based AODV protocol.

Table 6: Average End-to-End delay obtained by Proposed OBHA detection, PSO, and ABC based AODV protocols against number of nodes

Number of Nodes	Average End-to-End delay (Seconds) by AODV protocols		
	Proposed OBHA	PSO	ABC
10	0.08	0.17	0.11
20	0.12	0.21	0.19
30	0.18	0.29	0.24
40	0.25	0.32	0.31
50	0.34	0.44	0.39
60	0.45	0.58	0.55
70	0.52	0.71	0.63
80	0.61	0.86	0.82

6. CONCLUSION

Concerns about computer network protection have been extensively debated and popularised in recent years. However, the conversation has traditionally focused on static and wired networking, with mobile and ad-hoc networking problems receiving little attention. Since mobile ad-hoc networks (MANET) vary greatly from wired networks, the advent of such new networking techniques poses new challenges also for the fundamentals of routing. One of the security attacks that occur in mobile ad hoc networks is the black hole issue. During the route detection method in a Black hole attack, a spiteful node promotes that it has the best path to the target node. When it receives a Route Request (RREQ) packet, it broadcasts a false RREP to the resource node right away. The source node obtains the Route Reply (RREP) from the spiteful node first, before receiving all other RREPs. When the source node starts broadcasting the information packet to the end using this path, the spiteful node drops all packets instead of forwarding no information. This will degrade the network's lifespan and the setup's recollection. Optimization strategies such as PSO and ABC are combined in this study to detect single black hole nodes in the MANET. The proposed OBHA is evaluated using various evaluation metrics such as Packet Delivery Ratio, Detection Rate, Throughput, Average End-to-End Latency, and Routing Overhead in AODV routing protocol with PSO and ABC dependent single black hole node detection. When compared to existing optimization-based AODV routing protocols, the proposed OBHA approach reduced routing overhead, average latency, and improved packet delivery ratio, detection rate, and throughput, according to the results.

REFERENCES

[1] Nasipuri, Asis, Robert Castaneda, and Samir R. Das. "Performance of multipath routing for on-demand protocols in mobile ad hoc networks." Mobile Networks and applications 6.4 (2001): 339-349.

[2] Bhattacharyya, Aniruddha, et al. "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques." URL: arxivweb3. library. cornell. edu/pdf/1111.4090 (2011).

[3] Mishra, Amitabh, and Ketan M. Nadkarni. "Security in wireless ad hoc networks." The handbook of ad hoc wireless networks. 2003. 499-549.

[4] Pascoe-Chalke, Michael, et al. "Route duration modeling for mobile ad-hoc networks." Wireless Networks 16.3 (2010): 743-757.

[5] Begum, Syed Atiya, L. Mohan, and B. Ranjitha. "Techniques for resilience of denial of service attacks in mobile ad hoc networks." Proceedings published by International Journal of Electronics Communication and Computer Engineering 3.1 (2012).

[6] Xing, Fei, and Wenye Wang. "Understanding dynamic denial of service attacks in mobile ad hoc networks." MILCoM 2006-2006 IEEE Military Communications conference. IEEE, 2006.

[7] Vishnu, K., and Amos J. Paul. "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks." International Journal of Computer Applications 1.22 (2010): 38-42.

[8] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual Southeast regional conference. 2004.

[9] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of co-operative black hole attack in MANET." J. Networks 3.5 (2008): 13-20.

[10] Gupta, Prakhar, et al. "Reliability factor based AODV protocol: Prevention of black hole attack in MANET." Smart Innovations in Communication and Computational Sciences. Springer, Singapore, 2019. 271-279.

[11] Sivanesh, S., and VR Sarma Dhulipala. "Accurate and cognitive intrusion detection system (ACIDS): a novel black hole detection mechanism in mobile ad hoc networks." Mobile Networks and Applications (2020): 1-9.

[12] Elmahdi, Elbasher, Seong-Moo Yoo, and Kumar Sharshembiev. "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks." Journal of Information Security and Applications 51 (2020): 102425.

[13] Rameshkumar, S. G., and G. Mohan. "Detection and Avoidance of Single and Cooperative Black Hole Attacks Using Packet Timeout Period in Mobile Ad hoc Networks." Intelligent Computing in Engineering. Springer, Singapore, 2020. 625-634.

[14] Cherkaoui, Badreddine, Abderrahim Beni-hssane, and Mohammed Erritali. "Variable control chart for detecting black hole attack in vehicular ad-hoc networks." Journal of Ambient Intelligence and Humanized Computing 11.11 (2020): 5129-5138.

[15] Kumar, Ankit, et al. "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm." Microprocessors and Microsystems 80 (2021): 103352.

[16] Aranganathan, A., C. D. Suriyakala, and V. Vedanarayanan. "Discovery and Deterrence of Black Hole Attack in Clustering Ad Hoc Networks Based on Software Agents." Soft Computing Techniques and Applications. Springer, Singapore, 2021. 681-689.

[17] Bhardwaj, Suyash, and Vivek Kumar. "Secure co-operative neighbour-based approach for detection and prevention of black hole attack in wireless mobile ad-hoc networks." International Journal of Wireless and Mobile Computing 19.1 (2020): 62-72.

[18] Gayathri, V. M., and P. Supraja. "Optimised RBIDS: detection and avoidance of black hole attack through NTN communication in mobile ad hoc networks." International Journal of Computer Aided Engineering and Technology 13.1-2 (2020): 4-13.

[19] Khan, Dost Muhammad, et al. "Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique." Information Technology and Control 49.3 (2020): 308-319.

[20] Ponnusamy, Muruganantham. "Detection of Selfish Nodes Through Reputation Model in Mobile Adhoc Network-MANET." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.9 (2021): 2404-2410.

[21] Subhashini, M., & Gopinath, R., Mapreduce Methodology for Elliptical Curve Discrete Logarithmic Problems – Securing Telecom Networks, International Journal of Electrical Engineering and Technology, 11(9), 261-273 (2020).

[22] Upendran, V., & Gopinath, R., Feature Selection based on Multicriteria Decision Making for Intrusion Detection System, International Journal of Electrical Engineering and Technology, 11(5), 217-226 (2020).

[23] Upendran, V., & Gopinath, R., Optimization based Classification Technique for Intrusion Detection System, International Journal of Advanced Research in Engineering and Technology, 11(9), 1255-1262 (2020).

[24] Subhashini, M., & Gopinath, R., Employee Attrition Prediction in Industry using Machine Learning Techniques, International Journal of Advanced Research in Engineering and Technology, 11(12), 3329-3341 (2020).

[25] Rethinavalli, S., & Gopinath, R., Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks, International Journal of Advanced Research in Engineering and Technology, 11(12), 3348-3356 (2020).

[26] Rethinavalli, S., & Gopinath, R., Botnet Attack Detection in Internet of Things using Optimization Techniques, International Journal of Electrical Engineering and Technology, 11(10), 412-420 (2020).