A Novel Survey on Comparison of Blackhole Attack Detection Techniques

Kavita S. Kumavat [1], and Yash Yadhav [2]
[1] Assistant Professor, Computer Engg. Dept, Vishwakarma University, Pune, Maharashtra, India
[2] Student, Computer Engg. Dept., Vishwakarma University, Pune, Maharashtra, Pune
E-mail: kavita.kumavat@vupune.ac.in

Abstract

Black hole attacks occur when a hacker takes control of a collection of nodes, modifies their programming, and blocks packets from being forwarded to the base station. This results in data being grabbed and traveling to the attacker's (black hole) area. By separating the network, these attacks are easy to develop and have the potential to reduce system efficiency, preventing base stations from receiving crucial information. Blackhole nodes can cause parameters of network performance such as throughput and end-to-end delay to change, with throughput falling and end-to-end delay rising. This paper highlights the efficiency and limitations with a comparative analysis of all existing approaches. This paper illustrated results using the AODV protocol for black hole attack detection using the Cuckoo search algorithm. The network is created for 15 nodes using a network simulator.

Keyword: Blackhole, Attack, Security, Network-Simulator, Detection.

1. Introduction

In the absence of a centralized controller, MANETs (Mobile Ad-hoc Networks) are mobile node networks that communicate with one another by sending data packets over multiple hops. Ad-Hoc On-Demand Distance Vector Routing Protocol is a sort of reactive routing protocol that constructs routes according to requirements rather than maintaining existing ones. These networks are made up of a moveable number of mobile hosts that communicate with one another using wireless links. Due to the lack of infrastructure in this network, nodes can move in any direction with any kind of mobility. As a result, there is also no central authority. Because to these characteristics, each node in this system functions as a router, sending data packets via the host. Like in wired or wireless structures, where some issues related to rotten and congested remains present frequently, the MANET offers various excellent explanations. We intend to modify established AODV protocols in light of the literature research to significantly improve the system's ability to mitigate blackhole nodes. Ad-hoc on-demand vector protocol is one of the most used routing protocols in Mobile Ad-hoc network systems, including low bandwidth sensors, Internet of Things devices, and non-centralized network devices[1]. Even yet, the AODV protocol is vulnerable to numerous security vulnerabilities, including selfish, flooding, and Greyhole attacks. In the MANET system, the black hole assault is the most frequent attack Also, it is challenging to identify and neutralize the danger. For this reason, in this project, we will examine AODVs from a security perspective and propose a new methodology that effectively locates and eliminates the black hole nodes from the system. A rogue node presents itself in this attack as having the network's shortest path to other nodes. We are going to use ns2 as a platform to detect blackhole attack on.

2. Literature Survey

This study suggests a strategy for identification and prevention. End-to-end delay and throughput during the experimental evaluation were both significantly impacted by the blackhole attack [1]. In most of the papers, authors used trust-based routing methods for blackhole attack detection [2]. The black hole and its preventive strategy employing ADOV with the shortest distance are built in the suggested system using NS2 (Network Simulator 2) [3]. The authors of this work suggested a technique for detecting black hole nodes in the sensor field. their technique divides the sensor field into zones that are the same size during the zone generation step [4]. After packets travel from the source to the sink node, it is noticed that the density curve drops concerning time and that it does not drop concerning time once packets travel from the source to the sink node [5]. They have suggested an energy-efficient intrusion detection method to protect network nodes from black hole attacks. Our method is straightforward and is based on the transmission of control packets between the base station and the sensor nodes [6]. In this study, the watchdog technique is used. By excluding the rogue node from the network, the suggested model enhances network performance [7]. Initially, an AODV protocol without an attack is built, and then we have a plan to stop the same network from being affected by a malicious node. When the AODV protocol implements a malicious node [8]. The routing table is included in the proposed methodology for detection. Compared to previous approaches, this one requires fewer cryptographic procedures for authentication [9]. The usage of clustering extends the life of the sensor nodes and lowers their battery consumption [10]. This paper does a thorough analysis of the cooperative black hole attack. Black holes attack in groups, which reduces throughput and lengthens delays [11]. The SENMA network authentication mechanism and design are utilized to find any blackhole nodes that may be present [12]. The suggested black hole alleviation method uses a mechanism to proactively identify the black hole nodes and isolate them to ensure secure communication [13]. As part of the suggested method, the data is first encrypted before being sent to the target node [14]. Two potential solutions are presented in the paper. Finding multiple routes to the destination is the first step. The second is to make use of the packet header's packet sequence number [15]. Using the leach protocol, we have suggested a defense method in this research against blackhole attacks on sensor networks [16]. Via simulation, they proved that their techniques could effectively and efficiently identify black hole attacks without adding a lot of routing control costs to the network [17]. To define the normal state of the network, they have created the feature and studied the blackhole attack in this study [18]. They will utilize a "Fidelity Table" to combat the black hole attack, and each participating node will be given a fidelity level that serves as a gauge of that node's dependability [19]. By using the node's sequence number to identify it, the proposed method can be utilized to locate secure routes and prevent black hole nodes in the MANET [20]. By putting bait timers in each node, the authors of [21] suggested a method for finding black hole nodes. The timing for the baiting is set to a random number. When the baiting timer reaches the predetermined time, fake ID broadcasts start to run. The black hole is configured to respond to every request, regardless of its purpose, therefore it responds to requests that are used as bait. As a result, the transmitting node finds the black hole node and keeps track of it in a particular table. Malicious nodes are ignored when the real requests are sent out under the data kept in the malicious node database. In [22], the authors suggested a node activity-based trust and reputation estimate (NA-TRE) approach to track the node's actions, classify them as legitimate (N) or malicious (M), and calculate the estimation of trust and reputation. There are three states of nodes, according to the author: a normal state (NS), where nodes make every effort to cooperate and follow routing requirements; a resource limitation state (RS), where nodes are not cooperating as much due to low power consumption, being outside of communication range, or having high congestion, etc.; and a malicious state (MS), where nodes disrupt the network by starting denial of service attacks, creating new paths, delaying packets, or engaging in other malicious behavior. Prediction is performed based on a “Semi-Markov probability decision process” to proactively distinguish different states. Ad hoc on-demand multipath secure routing (AOMSR), an improved routing protocol, was put out by the authors in [23] and is based on acknowledgment. Based on the maximum data reception latency, this routing system requires a source node to maintain numerous pathways from

the source to the destination. As an alarm system, an intrusion detection system operates. It sends a warning to the system when it finds an attack [24]. The IDS system has an audit register where all the data is kept for analysis and outputs are given from which judgments are made.

TABLE 1: Comparative Analysis of existing system

Author	Method	Advantages	Disadvantages
(Abdullah Aljumah et al)	Basic network parameters and novel approach.	Blackhole attack influence is quantified.	It is not an effective strategy since system stability is compromised as the number of attackers rises.
Mandal	Trust-based routing	High trust value nodes have less packet loss. QoS is elevated.	There is more network delay.
(Nigahat et al)	Distance Vector Protocol based approach .	PDR and delay-based evaluation yield superior outcomes.	Because of the high cost, a MANET environment is not appropriate.
(Dr. Shreenath K N et al)	Concept of Mobile Agent approach	Applicable only in zone based wireless system	No prevention method is described.
(Mehndi Shamra et al)	Contingency approach	By Using a density curve with respect to time, blackhole attack can identify the malicious node.	No preventative measure is mentioned. Only relevant for the AODV network.
(A.Babu Karuppiah et al)	Improvised hierarchal vitality efficient IDS based method .	A straightforward method to recognise and stop black hole attacks	Not an efficient mechanism.
(Umashankar Ghugar et al)	Watchdog Monitoring Technique	blackhole attack detection and prevention enhances network performance.	Applicable only for AODV protocol.

(Vinod Bhupathi et al)	Trust Based Mechanism	With secure AODV, blackhole node detection is achievable. Secure data communication is provided.	NS2 simulator is used where bugs are not reliable.
(Anjali P.Rathod et al)	Routing Table base approach	Reduces cryptographic operation for authentication.	No prevention method is described.
(Kalaiselvan.K et al)	Monitoring fake packet replays based approach	Blackhole attacks can be recognised using threshold performance.	It is difficult to set threshold value
(Garima Gupta et al)	Cross Checking Algorithm	Cooperative blackhole attack is covered in great detail.	An inefficient approach since the delay value is constant throughout. Nevertheless, throughput has barely increased.
(Dr. Sharvani G.S et al)	Authentication Mechanism and qout-of-m rule based apprach	It is feasible to establish a secure connection between source and destination using authentication mechanisms.	No prevention method is given.
(M.Rajesh B et al)	Alleviation Procedure	Different protocols are used to test the WSN's susceptibility to blackhole and other attacks. The best performance of blackhole attack resistance is shown by the SAR protocol.	In addition to the SAR procedure, they also have a number of other issues.
(Mehak Kaushal et al)	HOOSC Scheme based approach	A straightforward strategy is utilised to lessen the impact of a blackhole attack. A technique of preventive is also explained.	It is not a reliable technique for data security.

Al-Shur man	to discover multiple routes and take advantage of the packet sequence number.	Redundancy in the network is used to confirm the node's legitimacy. Quick and accurate in spotting a phoney response. No overhead is present.	The source node waits for all of the RREP packets, which causes a longer time delay. There are fewer paths that have been chosen.
(Vipul Sharma et al)	LEACH protocol based approach	Detection method is energy efficient	Security is an issue since all an attacker has to do is launch an attack against the base station.
Bo Sun	Neighbor hood-based method and routing recovery protocol	Identify black hole node misbehaviour. There are fewer cryptography operations now.	It costs money to retrofit security measures. There is no increase in packet throughput. It is ineffective to route control traffic.
(Satoshi K et al)	Detection System approach Based on anomaly	The outcome of the simulation makes it obvious whether or not there is a blackhole attack on the network.	No prevention method is provided.
Tamilsel van	Fidelity table	Performance and security are improved.	There is additional network delay. There is higher routing overhead.
Himral	Sequence num ber concept.	To ignore control messages coming from the malicious node, MN-Id is kept as its identification.	The network's performance is not examined. can't stand up to several black hole nodes.

These are analyses for 20 published Research Papers, in which the name of the author, the method used, and Advantages and Disadvantages of the respective papers are specified.

3. Methodology

3.1. System Overview:

System overview represents details about system flow as well as different considerations of the system. In system overview, we study the concept of blackhole attack, Network Simulator, and AODV protocol details.

Basic Details

A. Black-Hole Attack

A rogue node presents itself in this attack as having the network's shortest path to other nodes. But, instead of forwarding packets to their intended destination when they are received with a destination of another node, it drops them. The malicious black hole node in our simulation scenario sends a Route Reply packet to the destination every time it receives a Route Request packet without first verifying that it actually has a path to the desired destination. So, whenever a Routing Request packet is received, the black-hole node is the first node to answer. Furthermore, if the packets are headed for other nodes, the malicious node drops every Route Reply and Data packet it gets.

1. The highest sequence number with the least number of hops.

2. Updating of the incorrect route message in the route table.

3. Wired Connection

4. Using strategies used by other security threats, such as wormhole attacks.

B. NS2 Details

An open-source, event-driven simulator called Network Simulator 2 (NS2) was created especially for the study on computer communication networks.

Since it was intercepted in 1989, NS2 has attracted a lot of attention from business, academia, and the government. After years of continuous research and development, NS2 now has modules for many different network elements, including routing, transport layer protocol, applications, etc. Researchers can easily configure a network using a simple scripting language to study results produced by NS2 to study network performance. Without question, NS2 has grown to be one of the most popular network simulators and the most commonly used open-source network simulator. On an NS-2 simulator, we have the Blackhole attack built. We use the IEEE 802.11b MAC, the CBR (Constant Bit Rate) application, TPC/IP (full duplex communication), and a physical channel based on a statistical propagation model for our simulations. In a flat area measuring 500 by 500 meters, 30 wireless nodes make up the simulated network. A 250-meter power range is the node transmission range. For instances involving node mobility, the random waypoint model is employed. The chosen pause duration is 30 seconds.

For simulating constant bit rate (CBR) sources, a traffic generator was created. The data payload is 512 bytes in size. In our example, there are 30 nodes total, with nodes 1 through 22 and 25 through 30 being basic nodes and nodes 23 and 24 being malignant or black hole nodes. Ns2 is used to simulate the network and study network performance by changing node mobility. These are the metrics that were utilized to assess performance.

Packet Delivery Ratio: The proportion of packets sent by "application layer" CBR sources to the number of packets the CBR sink receives at the destination.

Throughput: Throughput is known as the average rate of successfully delivered messages via a communication connection.

Node Mobility: Nodes' mobility speed is indicated by their node mobility.

C. AODV Protocol

Ad-Hoc On-Demand Distance Vector Routing Protocol is a sort of reactive routing protocol that constructs routes according to requirements rather than maintaining existing ones. The disadvantages of the Dynamic Source Routing Protocol and the Distance Vector Routing Protocol are addressed by AODV. Dynamic Source Routing is slow since it can keep track of the pathways between the source and the destination. It is challenging for the data packet header to carry all of the route information in a network with several routes connecting the source and destination. Several routes exist for sending a packet from source to destination in the case of dynamic source routing, although AODV also gets around this drawback. Sequence Number (SEQ NO) and broadcast ID are two counters that are maintained along with each node's routing tables in AODV.

3.2. System Workflow Diagram

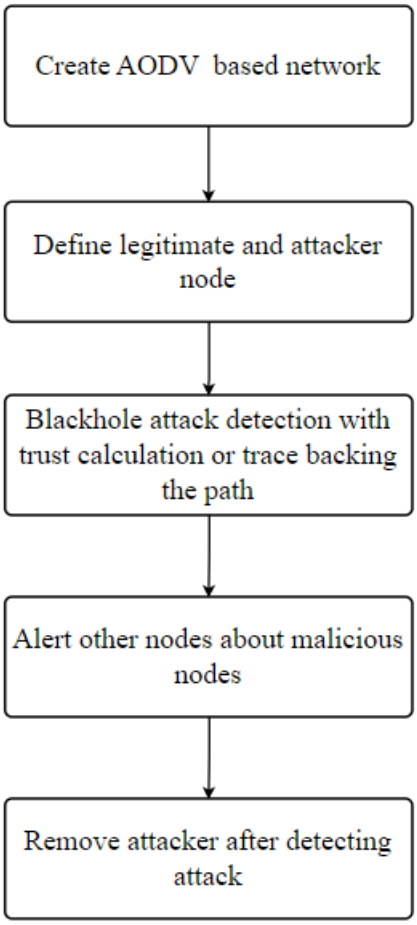

Figure 1: Blackhole attack detection workflow diagram

The first strategy that has been suggested is based on how malicious nodes behave in the network. Ad-hoc mobile networks with a constrained number of nodes will be deployed first. We'll use a very reliable node in the

MANETs—we'll call it the "IDS node"—to find a malicious node. The network's IDS node, or node within the network, needs to be established. The node with the greatest stability and the inability to often alter its location is the IDS node. The IDS node begins building each node's profile; it senses its neighboring node and stores its neighbor's information. The packet type—whether a control packet or a data packet is sent—is stored information. The packet type, whether it sends control or data packets, the data rate of sending packets (CBR or VBR), and threshold values are all stored information.

The beginning node will also examine route requests, and if it discovers the node that forwards the fewest packets, it will examine the time of the route request packet; otherwise, it will create a path from source to destination. If the route request packet arrives in the quickest time possible, the ids node will either label the route request initiate node as a malicious node or create a new path from the source to the destination. It will trace a path from the starting point of the data packets after building a path. The communication will continue if the node is the same as the one listed in the packet header; otherwise, it will return to creating each node's profile. The IDS node analyses each node's past profile with the current profile once the network throughput is below threshold levels. The network will identify the mismatched profile node as a malicious node.

Results and Discussion

Please provide a comparative study on recent and related published reports

4. Implementation and Result

Implementation details contain all the description about the network simulator 2 system and node transmission. It represents the node's connectivity and transmission protocol detail.

4.1. Fake Routing Method

4.1.1. Deployment of Network:

TABLE 2: Simulation Parameters

Parameters	**Value**
Number of nodes	15
Area	800 * 800 meters
Size of Queue	50
Link Layer	LL

The wireless ad hoc network is deployed with 15 mobile nodes. The reactive routing protocol is used in the network for the path establishment of which AODV routing protocol. The source and destination nodes are defined in the network for the data transmission, which is 0 and7. The source node flood route requests packets in the network from destination path to destination. The two parameters will be counted for the path establishment, which are hop count and sequence number.

4.1.2. The black hole attack simulation.

A black hole was produced by us. An example of a TCL script that simulates black hole attacks. The simulation was modified by adding the following settings, and we designated two nodes as our black hole nodes in the network.

So the node numbers 5 and 11 will be our malicious node and act as a black hole attack.

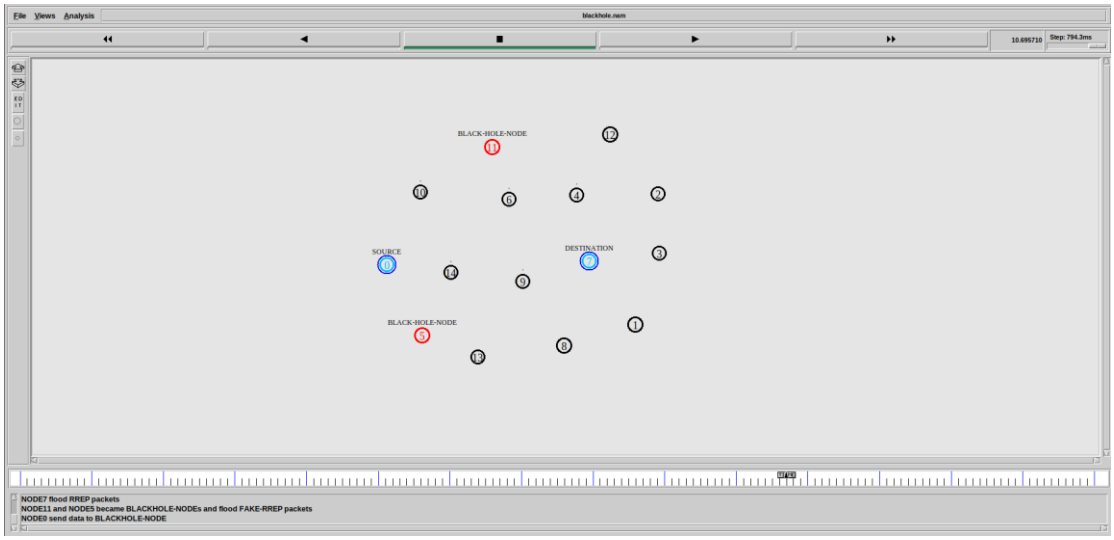

Figure 2 : Representation of Defined blackhole nodes

4.1.3. Identification of malicious node.

By requesting an unknown node that is randomly selected, we first start fake routing requests in the network. we set the nodes. So for node0, the source node that requests the fake route request and the malicious nodes will respond to this with a fake route reply. From that, we can identify these nodes as malicious.

4.1.4. ***Alerting all the nodes about the malicious nodes in the network.***In this phase, we will generate the alert as a broadcast message excluding the malicious node. We will tell other adjacent nodes that nodes 5 and node 11 are malicious in the alert message. After the alert, we will restore the communication.

Figure 3: Representation after alerting about malicious nodes.

4.2. Blackhole detection using Cuckoo Algorithm [22].

4.2.1. Cuckoo Search Algorithm

The cuckoo bird served as inspiration for the development of the Cuckoo search algorithm, a metaheuristic method. This bird rarely builds a nest of its own and typically lays its eggs in another bird's nest. Few host birds can directly confront the trespassing cuckoo. When the host bird discovers eggs that are not even their own, it either removes them from the nest, relieves the nest, or builds a new nest. Every egg in the nest portrays a solution, and the cuckoo egg presents a unique and superior one. The resultant solution is a fresh solution built on an existing solution that has had some of its properties changed. Cuckoo search is used in structural engineering to resolve scheduling challenges and design optimization problems. The breeding behavior is admired by cuckoo search, which can be developed for a variety of optimization issues, including those listed below:

1. Each cuckoo only ever lays one egg at a time, and she places it in a randomly chosen nest.

2. The higher egg-quality nests would pass on to the next generation.

3. There are only a limited number of open host nests, thus if a host bird discovers a cuckoo egg with a probability of page [0,1], it may throw or abandon the egg(s) and create a brand-new nest.

In order to improve routing discovery, Cuckoo Search Optimization is integrated into the AODV protocol in this study. Results for different node counts are calculated using NS2 to replicate the proposed method. Basic cuckoo search has been somewhat modified for the experiment for embedding and improved performance. Cuckoo search is built in C and is integrated into the route discovery section of NS2 because NS2 is compiled in C. Nodes with a higher sequence number and fewer hops are chosen in Vol. 1, Issue 1, July 2019 generic AODV. These nodes are chosen via cuckoo search following numerous iterations to guarantee the path efficiency. The following iteration finds a new path if efficiency is reduced. When a black hole attack occurs, cuckoo search drops the current path, finds a new one, and marks the malicious nodes to prevent further route discovery selection of those nodes. This happens when packets are not received by the intended destination.

Figure 4 : Representation of network without malicious node

Figure 5: Representation of network with malicious node

4.2.2. Results

TABLE 3: Performance evaluation of system with and without Blackhole attack for 20 Nodes

Nodes=20	No BH	with BH	Algo with BH
Throughput	51.44	32.51	51.32
PDR	99.59	30.75	74.54
END to END Delay	14.3	10.44	13.42
Packet loss	2.0090	339.325	124.754

We have compared the effects of black hole attack in respect of End to End Delay, Throughput, Packet delivery ratio, and Packet Loss in MANET and observed that improved algorithms has given better results in all ways.

TABLE 4: Performance evaluation of system with and without Blackhole attack for 25 Nodes

Nodes=25	No BH	with BH	Algo with BH
Throughput	51.21	14.65	27.66
PDR	99.19	21.18	53.53
END to END Delay	36.51	20.29	36.43
Packet loss	3.9689	386.218	227.703

5. Conclusion

In this paper, the AODV routing protocol was utilized in conjunction with the Cuckoo search optimization algorithm. The improved algorithm effectively thwarted the black hole attack. In terms of End-to-End delay, Throughput, Packet Delivery Ratio, and Packet Loss in MANET, we compared the impact of a black hole attack and discovered that the revised algorithm yielded superior results in all of these aspects. The proposed technique not only identifies and prevents attacks through its efficient network implementation but also significantly enhances network performance. Furthermore, it was observed that as the number of nodes in the network increased, the improvements yielded substantial outcomes. The research also suggests that the upgraded routing protocol will perform just as effectively as the standard AODV protocol in the absence of a black hole, even with an increased number of nodes.

6. References

1. A. Aljumah and T. A. Ahanger, “Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks,” vol. 17, no. 2, pp. 194–201, 2017.

2. Bar, R. K., Mandal, J. K., & Singh, M. M. (2013). QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack. Procedia Technology, 10, 530-537

3. “Nigahat, . Dinesh Kumar UCCA, Guru Kashi University, Talwandi Sabo UCCA, Guru Kashi University, Talwandi Sabo DOI : 10.5281/zenodo.546354,” vol. 6, no. 4, pp. 314–319, 2017.

4. K. N. Shreenath, “Black Hole Attack detection in Zone based Wireless Sensor Networks,” vol. 5, no. 4, pp. 148–151, 2017.

5. M. Samra and N. K. Gondhi, “Blackhole Attack Detection in Wireless Sensor Networks Using Support Vector Machine,” vol. 3, no. 5, pp. 48–52, 2016.

6. A. B. Karuppiah, J. Dalfiah, K. Yuvashri, and S. Rajaram, “An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks,” Int. Confernce Innov. Inf. Comput. Technol., no. Iceict, pp. 1–7, 2015

7. U. Ghugar, J. Pradhan, and M. Biswal, “A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol,” IJCSN Int. J. Comput. Sci. Netw. ISSN, vol. 5, no. 4, pp. 2277–5420, 2016.

8. V. Bhupathi, P. Priyanka, and G. S. Reddy, “DETECTION OF BLACK HOLE,” vol. 5, no. 2, pp. 305–311, 2016.

9. C. Engineering, A. P. Rathod, and N. A. Chavhan, “Detection Mechanism for Black hole attacks in,” vol. 5, no. 4, pp. 98–100, 2016

10. K. Kalaiselvan and G. Singh, “Detection and Isolation of Black Hole Attack in Wireless Sensor Networks,” vol. 4, no. 5, pp. 3516–3524, 2015.

11. G. Gupta and A. Mishra, “Simulation Based Study of Cooperative Black Hole Attack Resolution Using Cross- Checking Algorithm,” Int. J. AdHoc Netw. Syst. (IJANS), vol. 5, no. 2, pp. 17–28, 2015.

12. G. S. Sharvani, “Detection of blackhole attack in distributed wireless sensor networks,” pp. 172–175, 2015

13. M. R. Babu, S. M. Dian, S. Chelladurai, and M. Palaniappan, "Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version," Sci. World J., vol. 2015, 2015

14. M. Kaushal and G. Gandhi, "Detection Prevention and Mitigation of Black Hole Attack for MANET," vol. 4, no. 4, pp. 1431–1437, 2015.

15. Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp.96-97). ACM.

16. V. Sharma, K. Patil, and A. Tiwari, "Detection and Suppression of Blackhole Attack in Leach based Sensor Network," vol. 5, no. 6, pp. 1873–1877, 2014.

17. Sun, B., Guan, Y., Chen, J., & Pooch, U. W. (2003). Detecting black-hole attack in mobile ad hoc networks.

18. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," vol. 5, no. 3, pp. 338–346, 2007.

19. Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of co-operative blackhole attack in MANET. JNW, 3(5), 13-20.

20. Himral L., Vig V., & Chand N. (2011). Preventing aodv routing protocol from black hole attack. International Journal of Engineering Science and Technology (IJEST), 3(5), 3927-3932.

21. Yasin, A.; Abu Zant, M. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 9812135.

22. Ponnusamy, M.; Senthilkumar, A.; Manikandan, R. Detection of selfish nodes through reputation model in mobile adhoc network-MANET. *Turk. J. Comput. Math. Educ.* 2021, *12*, 2404–2410

23. Dave, D.; Dave, P. An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET. In Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, 24–27 September 2014; pp. 1690–1696.

24. Preet, M.P.; Mishra, R.; Agrawal, S. Research Technology Intrusion Detection System For Manet. *Int. J. Eng. Sci. Res. Technol.* **2020**, *6*, 402–406.

25. Hiren.T, "A Modified and secured Ad-hoc on-demand distance vector protocol (AODV) to defend blackhole attacks in Mobile Ad-hoc Network (MANET)".

26. M. sharma S. Gupta, S. Deswal, "Blackhole detection and prevention in AODV protocol using modified Cuckoo Search Algorithm", vol.1, no.1, 2019.