



**International Journal of Mobile Network Design and Innovation**

ISSN online: 1744-2850 - ISSN print: 1744-2869  
<https://www.inderscience.com/ijmndi>

---

**Black hole attacks recognition in wireless mobile ad hoc networks (MANET)**

A. Rajasekar, V. Kavitha, Hima Vijayan, Sheshang Degadwala

**DOI:** [10.1504/IJMNDI.2025.10070023](https://doi.org/10.1504/IJMNDI.2025.10070023)

**Article History:**

|                   |                  |
|-------------------|------------------|
| Received:         | 16 November 2024 |
| Last revised:     | 14 January 2025  |
| Accepted:         | 30 January 2025  |
| Published online: | 16 June 2025     |

---

## Black hole attacks recognition in wireless mobile ad hoc networks (MANET)

---

A. Rajasekar\*

Department of Artificial Intelligence and Data Science,  
Sri Sairam Institute of Technology,  
Sai Leo Nagar, West Tambaram,  
Chennai, 600044, Tamil Nadu, India  
Email: rajasekarbe@gmail.com  
\*Corresponding author

V. Kavitha

Department of Artificial Intelligence and Data Science,  
V.S.B. Engineering College,  
NH-67, Covai Road, Karudayampalayam Post,  
Karur, 639111, Tamil Nadu  
Email: kavithataru2015@gmail.com

Hima Vijayan

Department of Information Technology,  
S.A. Engineering College,  
Poonamallee-Avadi Road, Thiruverkadu,  
Chennai, 600077, Tamil Nadu, India  
Email: himavijayan@saec.ac.in

Sheshang Degadwala

Sigma University,  
Post Bakrol, Ajwa Road, Waghodia, Nimeta,  
Vadodara, Gujarat, 390019, India  
Email: sheshangdegadwala@gmail.com

**Abstract:** The properties of the mobile ad hoc network (MANET), such as the fast speed at which the network may be set up and the absence of the need for centralised administration, have led to the rising popularity of this network and its use in a variety of industries. One of the methods that are used to secure the network's safety is the implementation of intrusion detection systems, or IDSs. IDSs that are based on clustering have gained a lot of traction in this network owing to the benefits that they provide, such as adequate scalability. This paper presents a novel approach for use in MANETs that uses the K-nearest neighbour (KNN) algorithm for clustering. The goal of this algorithm is to identify black hole attacks. The cluster head will be determined using fuzzy inference, taking into account its history and the amount of energy that is still available.

**Keywords:** black hole attack; cooperative black hole attack; malicious node; packets.

**Reference** to this paper should be made as follows: Rajasekar, A., Kavitha, V., Vijayan, H. and Degadwala, S. (2025) 'Black hole attacks recognition in wireless mobile ad hoc networks (MANET)', *Int. J. Mobile Network Design and Innovation*, Vol. 11, No. 3, pp.152–162.

**Biographical notes:** A. Rajasekar is working as an Assistant Professor at Sri Sai Ram Institute of Technology, Chennai. He has completed his Bachelor of Engineering degree in Electronics and Communication Engineering from Anna University, Chennai. He has completed his Master of Technology in Embedded system Technologies from SRM University, Chennai. He has completed his PhD course in Hindustan Institute of Technology and Science, Chennai and indulged in research work in the field of cyber physical systems. His field of interest in the domain of embedded systems, communication networks and Internet of Things. He has overall teaching experience of over 13 years in the affiliated college under Anna University. He has published more than 15 research articles in refereed International and National journals in the areas like control systems, embedded systems, computer networks and internet of things, etc.

V. Kavitha has completed her ME in Computer Science and Engineering from the Anna University Trichy and currently working as an Assistant Professor in the Department of Artificial Intelligence and Data Science at V.S.B. Engineering College, Karur, Tamil Nadu, India. She has completed her Bachelor of Engineering in Computer science and Engineering from the Easwari Engineering College, Chennai. She has 18 years of teaching experience and has attended many FDP, online courses like Udemy, Coursera and conferences. Her area of interest includes cloud computing, data mining, data structures, artificial intelligence, machine learning and medical data.

Hima Vijayan is an Assistant Professor, Department of Information Technology, SA Engineering College, Chennai, India. She received her BTech in Computer Science and Engineering from Ilahia College of Engineering and Technology, Muvattupuzha, Kerala in 2008 and MTech in Computer Science with specialisation in Data Security from Toc H Institute of Science & Technology, Ernakulam in 2012. She has eight years of teaching experience. She is a life time member of Indian Society for Technical Education (ISTE). Her research interest includes data security, big data, artificial intelligence and cloud computing.

Sheshang Degadwala is presently working as an Associate Professor and the Head of Computer Engineering Department, Sigma University, Vadodara. He obtained his BE from the Department of Computer Engineering, BITs, Vadodara. Subsequently, he obtained his MTech from the Charusat University, Changa and his PhD in Computer Engineering from the Madhav University, Abu Road, Sirohi, Rajasthan, India in 2018. He has published 179 research papers in reputed international journals and conferences including IEEE, Elsevier and Springer. He is also Microsoft Certified in Python Programming and Excel. He has published 18 books and he got grant for one patent. He has published 38 Indian Patent. He has received 45 awards for academic and research achievement.

## 1 Introduction

Sharma and Gupta (2013), a mobile ad hoc network (MANET) is a sort of network in which the nodes may move around, the topology of the network can vary dynamically, and there is no permanent infrastructure. Within a MANET, the mobile nodes have the ability to join or leave the network at any moment. In addition, in order for them to interact with one another, they employ a wireless network that has many hops. In addition, MANET's nodes interact with one another via the use of routing protocols. Because of this, the nodes are able to determine the path that is the shortest between the source node and the destination node. Each mobile node in a multi-hop network also has the ability to function as a router during communication between two other mobile nodes in the network. Because it does not need a separate infrastructure to function, is capable of multi-hop communication, is transportable, and can adapt to changing conditions, MANET is applicable in a variety of contexts, including crises, automotive networks, meetings, and military operations. On the other hand, because of the characteristics of MANET, the nodes that make up the network are susceptible to a broad variety of assaults, including the black hole attack. The black hole attack is one of the many security risks that are present in MANETs. It is fairly frequent. As a result, it is essential for MANET to include detection and prevention mechanisms for black hole assaults. Passive and active attacks are the two primary categories that may be used to describe the majority of MANET-based assaults (Kumar et al., 2013).

In addition, the attacker has the capability of causing disruption to the process of routing by losing packets,

injecting packets, changing packets, and so on. It is necessary to have security systems in place in order to defend against a variety of assaults, such as a black hole in MANET. These techniques have been developed as a result of the findings of these research projects.

In Section 2, routing protocols are described, and a black hole attack in MANET is discussed. In Section 3, the scientific efforts that have been suggested to counter black hole attacks are discussed. The next section, Section 4, discusses research voids and potential future paths. The last section of the paper is concluded in Section 5.

### 1.1 Routing protocols and black hole attack

#### 1.1.1 Protocols used for routing

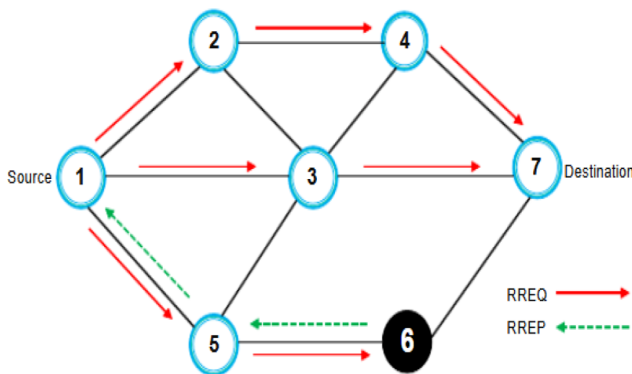
It is up to the routing protocols in a MANET to choose the communication route that will be the most time and resource effective in order to carry out communication between the source node and the destination node (Patel et al., 2014). The proactive, the reactive, and the hybrid approaches are the three basic categories that may be used to arrange them (Kaur et al., 2013; Kumar et al., 2010). In addition, each node is equipped with a routing table, and before sending a packet to another node, the sending node looks up the information in this database to identify which node will act as the next hop along the route leading to the destination node (Panos et al., 2017). The implementation of proactive routing protocols is best suited for use in network topologies that do not include a large number of nodes. In addition, reactive routing systems do not frequently provide topological information about the network via transmissions. Temporary ordered routing protocol

(TORA), ClusterBased routing protocol (CBRP), signal stability-based adaptive routing protocol (SSA), ad hoc on-demand distance vector routing (AODV), dynamic source routing (DSR), and associativity based routing (ABR) are all examples of reactive routing protocols (Khanna and Sachdeva, 2019). The proactive and reactive routing protocols are used to construct the hybrid routing protocol, which is formed by merging the characteristics of two distinct kinds of routing protocols. This routing strategy helps reduce the control traffic overhead that is caused by proactive systems by cutting down on the amount of unnecessary traffic. Another purpose of the hybrid routing protocol is the maintenance of a routing database, which allows it to cut down on the route discovery delays that are characteristic of reactive systems. This is made possible by the hybrid routing protocol's ability to reduce these delays. There are many different kinds of hybrid routing protocols, some of which include the dual-hybrid adaptive routing (DHAR) protocol, the adaptive distance vector routing (ADV) protocol, the zone routing protocol (ZRP) protocol, the sharp hybrid adaptive routing protocol (SHARP) protocol, and the neighbour-aware multicast routing protocol (NAMP) protocol (Goyal et al., 2011).

## 1.2 Black hole attack

One of the most common and potentially harmful techniques used by MANET is known as the black hole attack. The network layer is where this assault takes place. The black hole attack is shown in Figure 1 as an example. The phony RREP packet is sent back to the source node by an illegitimate node that is acting as a forwarding node and serving as a forwarding node.

**Figure 1** Artificial black hole attack: node 6 sends false RREP (see online version for colours)



## 2 Literature review

The authors of the paper (Jaiswal and Sharma, 2013) suggested a technique that protects against Encrypted route to the target node. A similar identification approach was suggested (Trivedi and Malhotra, 2019) in order to detect malicious nodes in MANETs. Cross verification was used in their study to detect rogue nodes. Additionally, a tracking system that can identify both black and grey hole assaults

was presented by the authors in paper (Nitnaware and Thakur, 2016). The remedy that they have suggested will take place in two stages. The suggested mechanism, on the other hand, results in increased computing complexity. The authors of the paper (Saurabh et al., 2017) provided a detection strategy for black hole attack that used a neuro fuzzy adaptive inference system (ANFIS) as well as particle swarm optimisation (PSO). In addition, a method for protecting oneself against assaults carried out by black holes was described in the work of Albalas et al. (2019). In order to protect the AODV routing protocol from being vulnerable to a black hole attack, Saurabh et al. (2017) suggested using a clustering mechanism. The nodes are arranged in clusters, and in the centre of each cluster is a node that serves as the head. In addition, the person who leads the cluster is chosen at random. Since MANET is a mobile network, there is a possibility that there may be some issues as a consequence of nodes leaving and joining other clusters. As a result, it can result in an incorrect detection of the black hole node. In order to protect against black hole assaults, the relief categorisation method was implemented (Arulkumaran and Gnanamurthy, 2019). During the online phase of the process, network nodes that have the previously described characteristics are commonly detected. If the value of a discovered network node is greater than a previously established threshold, then that node is considered to be malicious and is removed from the routes. A trust-based routing strategy was introduced by Veeraiah and Krishna (2019), as a means of protecting against black hole attacks. As part of its duties, each node is responsible (Veeraiah and Krishna, 2019) for preserving the trust value of its neighbouring nodes. The trust value is calculated in advance of the packet's actual transmission (Gurung and Chauhan, 2018).

Since the trust values are updated on a regular basis, their recommended method results in increased routing overhead. In addition, presented a detection strategy that would limit the effects of black hole assaults by employing fuzzy clustering and the Bayesian rule. The nodes are organised into clusters by the use of a fuzzy clustering approach, which centres on the ideal centroid, in the work that they have done. In addition, the node trust table includes all of the trust values that are connected to each individual node in the network. The detection mechanism performs an examination of the node trust database; if it determines that a node should not be trusted, the detection mechanism marks that node as an illegitimate node. Nevertheless, their recommended approach results in increased maintenance burdens. This method of detection is not suitable for usage in networks that have a significant number of mobile nodes since the nodes have a propensity to group together (Gurung and Chauhan, 2018).

After sending the SUSPECT packet into the network, the source node searches the detection module for an unauthorised node and then sends the ALERT packet out into the network. The reply from the illegitimate node is disregarded by the other nodes since it is not included in the process of route discovery that occurs inside the prevention

module. In addition to this, their detection method results in a significant increase in the routing overhead. In a similar manner, Singh and Hasan (2018) devised a technique to defend against attacks from black holes. They determined a value to use as a threshold and then checked RREP messages by utilising that determined value. The RREP messages' source node undergoes a destination sequence number check before they are sent. The node is considered to be malicious if the target sequence number is lower than the threshold value that has been established. The authors describe a method that changes the AODV routing protocol and enables a secured connection inside the network. Ndajah et al. (2019) However, since their suggested approach involves keys, it results in a significant increase in the amount of computing work that has to be done. The authors of the paper introduced the MBDP-AODV protocol, which is a protocol that defends against black hole attacks by using a dynamic sequence number threshold. Their procedure is broken up into three stages. During the initial step of the process, the source node makes use of the destination sequence number to calculate the mean and standard deviation. The problem is that their recommended method leads to a significant increase in routing overhead. The ALERT packets are being sent out onto the various networks. As a consequence, route reply from nodes that have been blacklisted is not allowed to occur. Their system contains a period for training and a phase for regular operation. During the training phase of the process, the cumulative sum method generates a random sequence denoted by  $X_n$ . This is then converted into a  $Z_n$  sequence that is completely random. A black hole assault is identified if the value of  $Y_n$  exceeds the threshold that is represented by  $N$ , regardless of the time period. Because of this, the usual phase will cause an alert to be triggered and will notify the other nodes on the network.

On the other hand, if an attack were to occur during the training phase of their detection system, it would not be possible to identify the assault since they would operate on the assumption that there was not an attack during the training period. In the paper the authors described a routing algorithm that is capable of sending falsified packets. A node is considered to be a black hole node if it answers to the source node while having a spoofed RREP packet in its possession. In addition, by sending a valid RREP message, it is isolated from the routing database of nodes that are part of the network. The authors in created a method for preventing black hole attacks using an algorithm that was based on dependability factor. The source node will continue to deliver a bogus RREQ if the dependability factor is less than 0.5. If a node provides a response, that node will be marked as a black hole node, and the attack will not be successful. In a similar manner, Pathan et al. (2019) devised a detection technique that detected black hole assaults by modifying the AODV routing protocol. The source node produces a bogus RREQ packet and sends it out across the network with a destination address that is not valid. Khan et al. (2020) developed a detection strategy that would limit the effects of a black hole assault by employing

a technique known as Ant Colony Optimisation. Similarly, the authors of Keerthika and Malarvizhi (2019).

The trustworthy authority conducts investigations and processes the information from all of the nodes in an automated fashion. The trustworthy authority will reorganise the nodes in the network if it finds any malicious ones. The authors of the paper provided a detection technique that mitigates and removes black hole nodes. As a result of their effort, a data control packet was developed, which checks the route followed by all nodes throughout all phases. In addition, every node has a black hole check table, which is used to determine which nodes may be relied upon. Ali Zardari et al. (2019) presented a dual attack detection strategy to identify black hole and grey hole assaults in MANET. The CDS approach that they use in their work results in the formation of tiny clusters of nodes inside the network.

If an IDS node has reason to believe that another node is acting maliciously, it will send a block message to every other node in the network. After then, all of the nodes cease talking with the one that is suspected of being malicious. In order to protect the AODV routing protocol from being exploited by black hole attacks, Yasin and Abu Zant (2018) included a timing mechanism and a baiting strategy. Within the framework of their operation, every node has a bait-timer that has a random setting of  $T$  seconds. A detection system known as Secure-DSR was presented as a means of mitigating the effects of black hole attacks and enabling more secure communication inside networks. Presented as a means of mitigating the effects of black hole assaults in. In there is a proposal for an Identification and Confirmation system that is meant to detect black hole assaults in MANET. After a black hole attack has been spotted, its authenticity may be verified by consulting the attack history database's archive of earlier assaults. In their research, Hossain et al. (2019) offered a cryptographic method as a means of protecting MANET against the black hole attack.

However, owing to the need of computing keys and ciphers, the suggested technique might result in a significant increase in the network's overall compute cost. In addition, the authors of the paper suggested a safe routing protocol known as SAODV as a means of protecting against black hole attacks. This is done so that the asking node may get the information it needs. When the initial request is received, a timer is then established in the Timer Expired Table. This is followed by the collection of further requests from other nodes.

The source node is the one that generates the challenge value and sends it to the destination node. The answer value is computed by the destination node once it has been given the challenge value. This computation is performed using the received challenge value in addition to additional secret values that have been produced. In addition, while maintaining the confidentiality of the secret data, concentrated their efforts on developing a more secure AODV. They came up with a system that they named MOSAODV to protect against attacks from black holes. The

MOSAODV protocol requires the source node to delay its response to the first RREP it receives. In order to stop more packets from coming from a malicious node, the MOSAODV protocol stores the identity of the node and makes sure it is never used again.

However, their suggested protocol leads to expensive computation and has the potential to potentially contribute to false positives. False positives occur when the proposed protocol incorrectly labels good nodes as harmful nodes. CBDAODV is the name of the detection technique that was presented by the authors in. In CBDAODV, a source node must receive at least two RREP packets from other surrounding nodes in order to function properly. In addition to this, it utilises a different path in order to verify the optimum route that was picked. This would be an effective way to solve the problem. The task that they do involves the source node calculating peak value as well as storing all RREP messages. Method requires a significant amount of processing and the examination of sequence numbers in relation to peak value in order to identify rogue nodes. It is also possible for it to result in false positives. Chavan et al. (2016) made modifications to AODV procedures in their research to protect against black hole assaults. The updated protocol makes use of two different message approaches for verification, each of which is delivered from the source node to the destination node.

It was suggested in that a safe AODV routing technique may be used to prevent and defend against black hole assaults. The malicious node makes use of the same protocol, it will be able to examine it and determine a validity value before beginning an assault. To protect against the threat of a cooperative black hole assault, Tamilselvan and Sankaranarayanan (2008) developed a protocol that they named PCBHA. When a source node broadcasts RREQ packets to its neighbouring nodes, the source node waits for the RREP packets that its neighbouring nodes send back to it. After selecting a neighbouring node in the area that has a higher fidelity level and ensuring that it surpasses a previously determined threshold value, it sends data packets to the node that will serve as the final destination. In addition to this, as soon as the destination node receives the packet, it immediately sends an acknowledgment back to the node that sent it. Dokurer et al. (2007) introduced an improved version of the AODV routing protocol that protects against black hole attacks. Their method, on the other hand, is susceptible to assaults using cooperative black holes. In Delkesh and Jamali (2019), the authors suggest a method of authentication that makes use of improved certificates. Nodes carry out the task of authenticating one another by generating certificates and distributing them to the nodes in the surrounding area. In addition to this, a public key is produced by them even if there is no authority that is centralised.

However, since their suggested approach involves the development and use of keys, it results in a significant increase in the amount of computing work required. The authors of the paper described a safe AODV routing

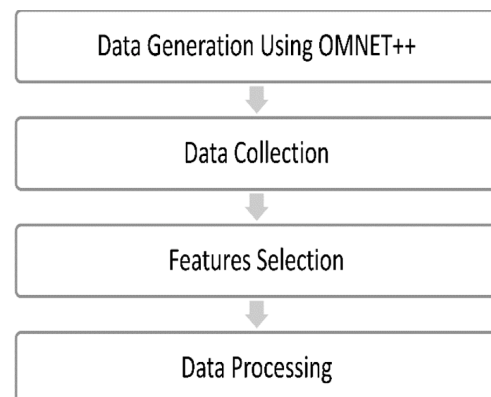
protocol that is capable of protecting against black hole attacks. In a similar fashion, Khanna (2016) developed a detection technique that protects against black hole attacks. Because it creates a trust hierarchy and encourages collaboration among genuine nodes, their work with the trueness level contributes to the prevention of packet drop assaults. In addition to this, their cryptography system makes it possible to keep information contained inside data packets secret. In addition to this, it assists with the authentication process and makes certain that there is encrypted connection between any two nodes. However, since the method requires the generation of keys, there is a significant amount of computational overhead involved.

Khanna (2016) proposed a TRACEROUTE method as a means of mitigating the source of a collaborative black hole assault. This method eliminates and flags the source of cooperation, which in turn breaks the collaboration that was taking place between the illegal nodes. Their approach, on the other hand, leads to unnecessary communication overhead. A protocol for achieving cooperative routing that is based on an altered version of AODV was suggested by Venkanna et al. (2015). The calculated values provide a trustworthy and cooperative path between a source node and a destination node. On the other hand, their method results in an increase in both the amount of energy that is used and the routing overhead.

### 3 Methodology

The methodology utilised in this study can be divided into four distinct components, all of which are illustrated in Figure 2. The traffic records that are gathered have a few similar aspects or qualities among themselves. A support vector machine (SVM) is used to conduct an analysis of these patterns in order to categorise the traffic as either benign or malicious. On the basis of this research, malicious nodes may be located and prevented from communicating.

**Figure 2** A black hole attack mitigation method from the study



#### 3.1 Solution

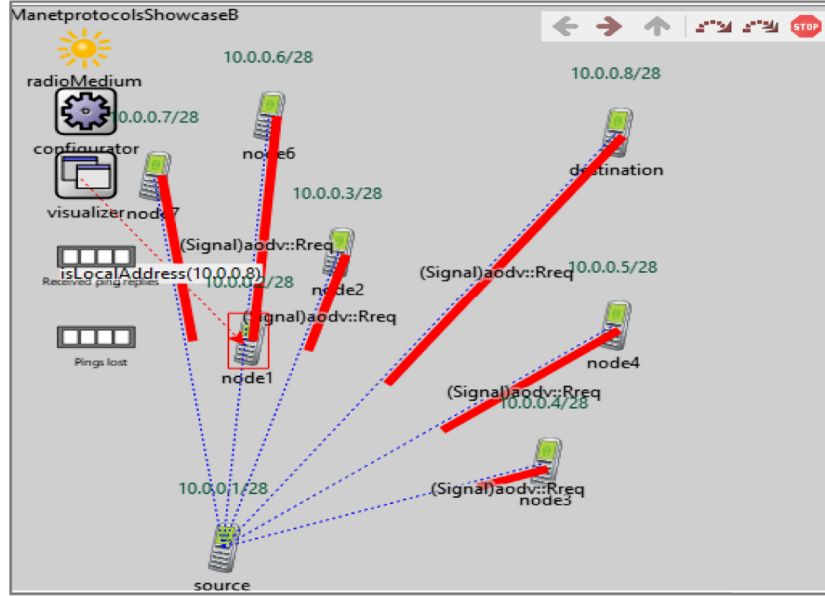
A blackhole assault corrupts MANETs. Studying malicious node activity in a network helps identify such assaults. There are several common behavioural traits:

- They boost the amount of power that their transmissions have in order to be able to reply to the majority of the RREQ.
- They practically never respond with any kind of RREQ.
- They never transmit anything and always use unicast exclusively.

### 3.2 The production of data

During this simulation, two different situations will be played out. The first scenario is a simulation in which all of the nodes work together and there are none that are malignant. A screenshot from OMNET++ depicting a node transmitting packets is presented in Figure 3.

**Figure 3** OMNET++ screenshot of a node transmitting packets (RReq) to neighbours (see online version for colours)



As presented in Table 1, the radio transmission power of Node 6 is initially set to 5 mW. By increasing its transmission power, Node 6 can mislead all its neighbouring nodes into perceiving it as their closest adjacent node.

**Table 1** OMNET++ simulator dataset generation parameter setting (Abdelhamid et al., 2023)

| Simulation environment parameters |            |
|-----------------------------------|------------|
| Simulation used                   | OMNET++ 57 |
| Number of nodes                   | 7 nodes    |
| Routing protocol                  | ADDV       |
| Total space                       | 400 m      |
| Transmission power (All nodes)    | 1 mW       |
| Transmission power (Node 6)       | 5 mW       |
| Transmission speed                | 24 Mbps    |
| Mobility speed                    | 25 mpt     |
| Transport protocol                | UDP        |

### 3.3 Data collection

Table 2 can be seen here. After that, the outcomes of the two different situations were sent through the detection system so it could do an analysis. The simulation was carried out in OMNET++, and the results were saved as a dataset with the most important data included.

**Table 2** OMNET++ simulator dataset generation parameter setting

| Dataset generated from OMNET++ |      |
|--------------------------------|------|
| Total number of records        | 8225 |
| Malicious traffic              | 2954 |
| Norinal traffic                | 5274 |

### 3.4 Feature selection

This study identifies three elements that contribute to the hostile behaviour of black holes. The aspect that comes in last, but certainly not least, is the fact that they never broadcast and always unicast.

### 3.5 The processing of data

Data from the OMNET++ simulator has eight columns. Five of the eight columns will be analysed, while three will be removed as useless. Five values are below:

- There are two ways that this paper adds to the study. The first thing it shows is the direction the signal is going in along with the node that was used as a hop, or the node that was in charge of directing communication.
- This part talks about the type of communication and how much power is being sent. There are two important numbers that it shows. The first is whether it is a route request (RReq) or a route reply (RRep). This is an important field that is used to find the nodes that are not

sending any RReqs. Additionally, this is one of the traits that shows incorrect behaviour, along with other traits.

- *Node name*: This field holds the name of the node that is sending the data. It is used to find the node that is acting in a bad way and to identify each node.
- *Transfer type*: This field has both the value of the transfer type and the value of whether it is broadcast or unicast. A lot of importance comes from the fact that this is used to show which nodes are not sharing. Keep an eye out for these nodes because, based on their other traits, they are most likely to act in a strange way.
- *Power of transmission*: This field displays the power of transmission that was used while sending the data. Because a black hole assault often results in an increase in the power of the node, it is very crucial to demonstrate whether or not there has been any manipulation of the power that is utilised for communication.
- The traffic will then be sent into a system like the one illustrated in Figure 4, where it will be analysed and an SVM machine learning algorithm will be used to identify malicious nodes based on the feature selection. Figure 4: The system that will process the data. The intrusion detection technique is illustrated in Figure 5.

**Figure 4** Malicious node behaviour-based feature selection

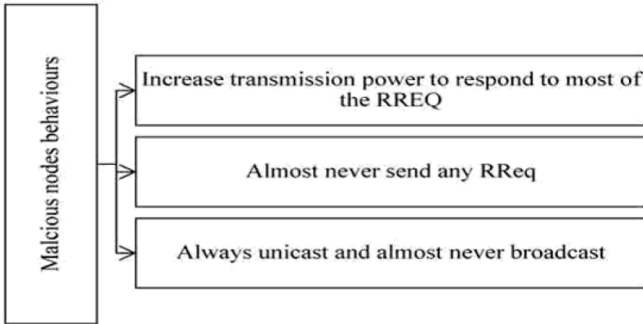
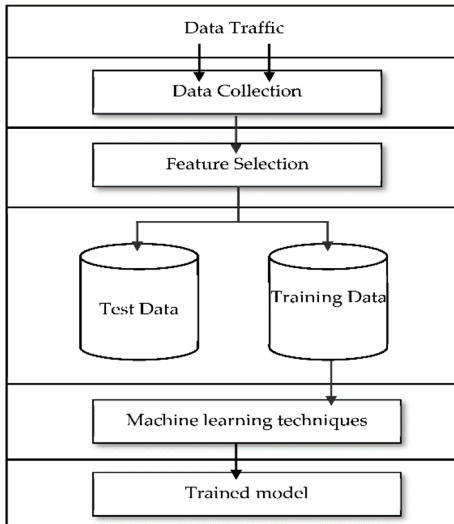


**Figure 5** Intrusion detection technique



### 3.6 Making use of machine learning (SVM)

Patterns may be divided into two distinct categories with the use of these lines (Ndajah et al., 2019; Jaiswal and Sharma, 2013; Vatambeti et al., 2020). Based on the examination of the data, this model is used in our situation in order to differentiate between nodes with regular behaviour and those with malicious intent:

$$D = \{(x_i, y_i)\}_{i=1}^n \quad (1)$$

The first class has a value of plus one (+1), whereas the second class has a value of minus one (−1). Even while there is leeway for some variation among characteristics and it is impossible for them to be exactly the same, they may still be properly defined. There is a predetermined margin that allows for some wiggle space in terms of what constitutes an acceptable deviation. As was discussed before, the line that passes through the centre of the figure is known as the optimum classification line.

$$\omega \cdot x + b = 0 \quad (2)$$

Due to the fact that the features of the vectors are not exactly the same, there are two additional lines that have some margin.

The term “hyperplane” refers to the plane that is formed by these two marginal lines. As seen in equation (3), the first class is comprised of the points that lie above the hyperplane:

$$\omega \cdot x + b > 1 \quad (3)$$

In a manner quite similar to the previous example, the points that are situated below the hyperplane are included in the second class, as shown by equation (4):

$$\omega \cdot x + b < 1 \quad (4)$$

In the following discussion, we will refer to these two categories as harmful vectors and normal vectors.

## 4 Results

The simulator was constructed so that it could explore the ways in which seven distinct nodes in the network communicated with one another. A rogue node that imitated an attack from a black hole was developed and included as one of the nodes in the network. It was given a total of seven minutes of time. The system looked at a total of 13,336 records, 13,336 of which were created by the simulation itself. The algorithm was finally successful in classifying the data into two distinct categories: those records that were not hazardous and those records that were. Out of the 13,336 records, there were a total of 10,381 records deemed to be normal, while there were 2954 records deemed to be harmful. This assertion was validated by the following three primary considerations:

- A change in the amount of power sent. As we’ve already talked about, the bad node will change the strength of its broadcasts to get close to the party sending the RReq.

This is a huge step forward in responding to as many RReqs as possible. The intrusion detection system technique is illustrated in Figure 9.

- Always use the unicast technique and send broadcast messages very rarely.

During the duration of our simulation, the radio transmission strength of Node 6 was increased to 5 mW, whilst the power of the other nodes was left at their usual, default value of 1 mW. This was done so that the results of our simulation would be more accurate. The second trait that sets the black hole attacker apart from other types of cybercriminals is the fact that they replied to the maximum amount of route requests (RReqs) while still keeping a status that was practically noticeable. The black hole attacker almost never broadcasted, opting instead to carry out all of its communication via the use of the unicast protocol. This is the last trait of the black hole attacker, but it is definitely not the least important. Figure 6 of the network presents a visual representation of the usual activities carried out by six separate nodes. The standard protocol is followed by all of them when transmitting RReqs and RReps. The results of the simulation in the absence of black hole attacks are presented in Figure 7.

**Figure 6** Support vector machine

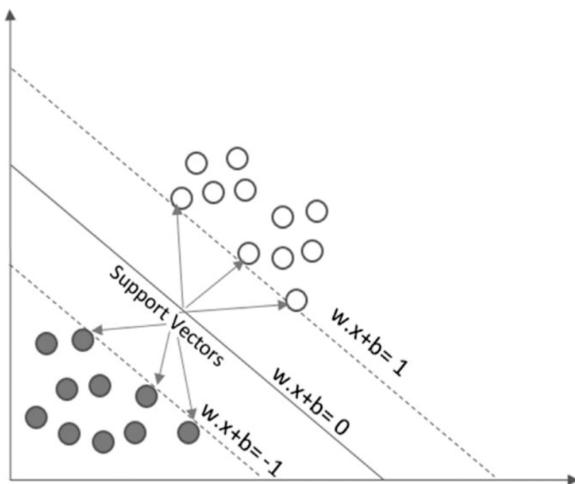


**Figure 7** Simulator results without black hole attacks (see online version for colours)

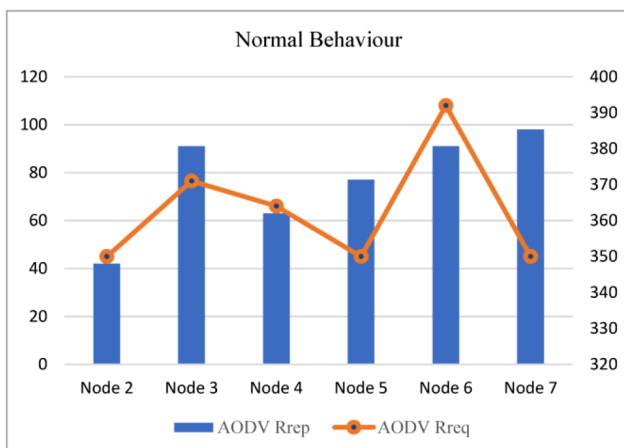


**Figure 8** Simulation results during a black hole assault (see online version for colours)

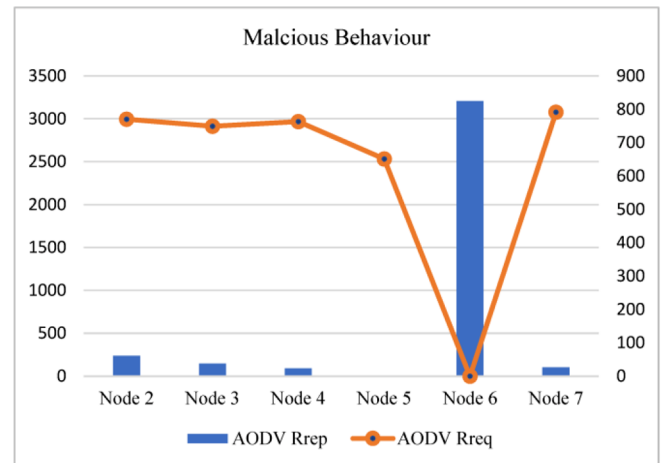


**Figure 9** Intrusion detection system technique (see online version for colours)

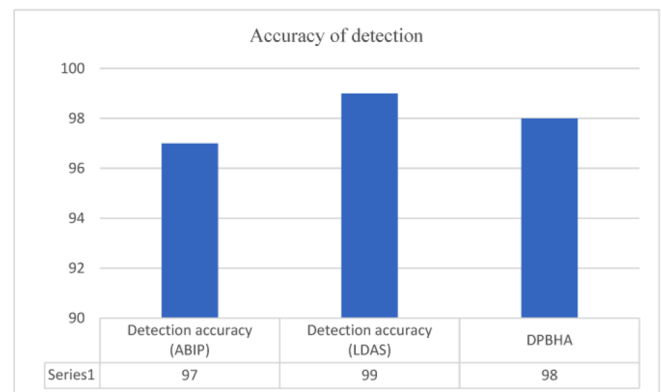


Figure 8 highlights a substantial gap in the RRep messages transmitted by Node 6 to other nodes. This discrepancy can be attributed to an increase in Node 6's transmission power to 5 mW, whereas the transmission power of the remaining nodes remained at 1 mW. As a result, Node 6 transmits very few RReq messages, while the other nodes, being in close proximity, generate a significantly higher number of RReq messages.

## 5 Conclusions

MANETs are a kind of network that do not rely on an underlying infrastructure to function. Instead, they are supported by the collaboration of its nodes, which act as both clients and routers. These networks are severely short in resources, in addition to a multitude of other security components. As a direct result of this, they are more susceptible to disruptions than the traditional infrastructure networks. In this paper, we covered a number of topics, including the many uses of MANETs, the issues encountered by their security, and the black hole assault, which is one of the most popular kinds of attack. In order to defend ourselves from black hole assaults, we carried out a comprehensive examination, categorization, and comparison of the many tactics that were suggested in the

mentioned scholarly literature. Following that, an approach that makes use of machine learning as its foundation was suggested as a method for locating and evading assaults of this kind. The term for this practice was “machine learning.” in order to mimic a rogue node on a MANET network, we made use of OMNET++. Because of this, we were able to generate a dataset that we could utilise for analysis and to investigate the actions of a malicious node that was carrying out a black hole assault. In addition to this, we were in a position to investigate the attributes of a malicious node that was carrying out an attack in the form of a black hole. As a result of this, we were able to carry out an in-depth investigation on attacks that used black holes. Transmission power, the number of answers as a fraction of the total number of nodes, and the communication mechanism were the three primary facets that we concentrated our attention on in order to detect black hole assaults. With the use of machine learning, a comprehensive investigation of these three characteristics was carried out. For the sake of this study, the simulation was only run on seven nodes, and the adversary was only modelled on one of those nodes. One of the issues with the research is that this occurred. It is possible that in the not too distant future it will be possible to establish a larger network for the purpose of carrying out more in-depth investigations, and the adversaries may consist of more than one node in the network. This is a possibility. Because of this, it will be possible to conduct an inquiry into black hole assaults inside a larger network, as well as an evaluation of network traffic even when there are numerous attacker nodes present in the network. In addition, this will make it possible to execute both of these tasks simultaneously.

## References

- Albalas, F., Yaseen, M.B. and Nassar, A.A. (2019) ‘Detecting black hole attacks in MANET using RELIEFF classification algorithm’, *Proceedings of the 5th International Conference on Engineering and MIS 2019*, 6 June, pp.1–6.
- Abdelhamid, A., Elsayed, M.S., Jurcut, A.D. and Azer, M.A. (2023) ‘A lightweight anomaly detection system for black hole attack’, *Electronics*, Vol. 12, No. 6, March, p.1294.
- Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K.H., Pathan, M.S., Hussain, M.I. and Memon, M.Q. (2019) ‘A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in manets’, *Future Internet*, Vol. 11, No. 3, p.61.
- Arulkumaran, G. and Gnanamurthy, R. (2019) ‘Fuzzy trust approach for detecting black hole attack in mobile adhoc network’, *Mobile Networks and Applications*, Vol. 24, No. 2, pp.386–393.
- Chavan, A., Kurule, D. and Dere, P. (2016) ‘Performance analysis of aodv and dsdv routing protocol in manet and modifications in aodv against black hole attack’, *Procedia Computer Science*, Vol. 79, pp.835–844.
- Delkesh, T. and Jamali, M.A.J. (2019) ‘Eadv: detection and removal of multiple black hole attacks through sending forged packets in manets’, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, No. 5, pp.1897–1914.
- Dokurer, S., Erten, Y.M. and Acar, C.E. (2007) ‘Performance analysis of ad-hoc networks under black hole attacks’, *Proceedings 2007 IEEE SoutheastCon 2007*, 22 March, IEEE, pp.148–153.
- Goyal, P., Parmar, V. and Rishi, R. (2011) ‘MANET: vulnerabilities, challenges, attacks, application’, *IJCEM International Journal of Computational Engineering & Management*, Vol. 11, No. 2011, January, pp.32–37.
- Gurung, S. and Chauhan, S. (2018) ‘A dynamic threshold based approach for mitigating black-hole attack in manet’, *Wireless Networks*, Vol. 24, No. 8, pp.2957–2971.
- Hossain, S., Hussain, M.S., Ema, R.R., Dutta, S., Sarkar, S. and Islam, T. (2019) ‘Detecting Black hole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET’, *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 6 July, IEEE, pp.1–7.
- Kaur, H., Sahni, V. and Bala, M. (2013) ‘A survey of reactive, proactive and hybrid routing protocols in manet: a review’, *Network*, Vol. 4, No. 3, pp.498–500.
- Keerthika, V. and Malarvizhi, N. (2019) ‘Mitigate black hole attack using hybrid bee optimized weighted trust with 2-opt aodv in manet’, *Wireless Personal Communications*, Vol. 106, No. 2, pp.621–632.
- Khan, D.M., Aslam, T., Akhtar, N., Qadri, S., Rabbani, I.M. and Aslam, M. (2020) ‘Black hole attack prevention in mobile ad-hoc network (manet) using ant colony optimization technique’, *Information Technology and Control*, Vol. 49, No. 3, pp.308–319.
- Khana, N. (2016) ‘Mitigation of collaborative blackhole attack using traceroute mechanism with enhancement in aodv routing protocol’, *International Journal of Future Generation Communication and Networking*, Vol. 9, No. 1, pp.157–166.
- Khanna, N. (2016) ‘Avoidance and mitigation of all packet drop attacks in MANET using enhanced AODV with cryptography’, *MECS IJ Computer Network and Information Security*, Vol. 4, April, pp.37–43.
- Khanna, N. and Sachdeva, M. (2019) ‘A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in manets’, *Computer Science Review*, Vol. 32, pp.24–44.
- Kumar, G.V., Reddy, Y.V. and Nagendra, M. (2010) ‘Current research work on routing protocols for manet: a literature survey’, *International Journal on Computer Science and Engineering*, Vol. 2, No. 3, pp.706–713.
- Kumar, J., Kulkarni, M. and Gupta, D. (2013) ‘Effect of black hole attack on manet routing protocols’, *International Journal of Computer Network and Information Security*, Vol. 5, No. 5, p.64.
- Ndajah, P., Matine, A.O. and Hounkonnou, M.N. (2019) ‘Black hole attack prevention in wireless peer-to-peer networks: a new strategy’, *International Journal of Wireless Information Networks*, Vol. 26, No. 1, pp.48–60.

- Nitinaware, D. and Thakur, A. (2016) 'Black hole attack detection and prevention strategy in DYMO for MANET', *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, 11 February, IEEE, pp.279–284.
- Panos, C., Ntantogian, C., Malliaros, S. and Xenakis, C. (2017) 'Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks', *Computer Networks*, Vol. 113, pp.94–110.
- Patel, D.N., Patel, S.B., Kothadiya, H.R., Jethwa, P.D. and Jhaveri, R.H. (2014) 'A survey of reactive routing protocols in MANET', *International Conference on Information Communication and Embedded Systems (ICICES2014)*, 27 February, IEEE, pp.1–6.
- Pathan, M.S., He, J., Zhu, N., Zardari, Z.A., Memon, M.Q. and Azmat, A. (2019) 'An efficient scheme for detection and prevention of black hole attacks in AODV-based MANETS', *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 1, pp.243–251.
- Saurabh, V.K., Sharma, R., Itare, R. and Singh, U. (2017) 'Clusterbased technique for detection and prevention of black-hole attack in manets', *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)*, Vol. 2.IEEE, pp.489–494.
- Sharma, S. and Gupta, A.K. (2013) 'A comprehensive study of DYMO routing protocol', *International Journal of Computer Applications*, Vol. 73, No. 22, January.
- Singh, A. and Hasan, M. (2018) 'An improved mechanism to prevent blackhole attack in MANET', *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2016*, Springer, Singapore, Vol. 1, pp.511–520.
- Tamilselvan, L. and Sankaranarayanan, V. (2007) 'Prevention of blackhole attack in MANET', *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, 27 August, IEEE, pp.21–21.
- Trivedi, M.C. and Malhotra, S. (2019) 'Identification and prevention of joint gray hole and black hole attacks', *International Journal of Ambient Computing and Intelligence (IJACI)*, Vol. 10, No. 2, pp.80–90.
- Veeraiah, N. and Krishna, B.T. (2019) 'Trust-aware fuzzyclus-fuzzy nb: intrusion detection scheme based on fuzzy clustering and Bayesian rule', *Wireless Networks*, Vol. 25, No. 7, pp.4021–4035.
- Venkanna, U., Agarwal, J.K. and Velusamy, R.L. (2015) 'A cooperative routing for manet based on distributed trust and energy management', *Wireless Personal Communications*, Vol. 81, No. 3, pp.961–979.
- Yasin, A. and Abu Zant, M. (2018) 'Detecting and isolating black-hole attacks in MANET using timer based baited technique', *Wireless Communications and Mobile Computing*, Vol. 2018, No. 1, p.9812135.
- Deshmukh, S.R., Chatur, P.N. and Bhopale, N.B. (2016) 'AODV-based secure routing against blackhole attack in MANET', *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 20 May, IEEE, pp.1960–1964.
- Dorri, A., Vaseghi, S. and Gharib, O. (2018) 'Debh: detecting and eliminating black holes in mobile ad hoc network', *Wireless Networks*, Vol. 24, No. 8, pp.2943–2955.
- El-Semary, A.M. and Diab, H. (2019) 'Bp-aodv: blackhole protected aodv routing protocol for manets based on chaotic map', *IEEE Access*, Vol. 7, pp.95197–95211.
- Gupta, P., Goel, P., Varshney, P. and Tyagi, N. (2019) 'Reliability factor based AODV protocol: prevention of black hole attack in MANET', *Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018*, Springer, Singapore, pp.271–279.
- Gurung, S. and Chauhan, S. (2019) 'A dynamic threshold based algorithm for improving security and performance of aodv under black-hole attack in manet', *Wireless Networks*, Vol. 25, No. 4, pp.1685–1695.
- Jaiswal, R. and Sharma, S. (2013) 'A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network', *2013 3rd IEEE International Advance Computing Conference (IACC)*, 22 February, IEEE, pp.499–504.
- Lo, N.W. and Liu, F.L. (2013) 'A secure routing protocol to prevent cooperative black hole attack in MANET', *Intelligent Technologies and Engineering Systems*, Springer, New York, pp.59–65.
- Lu, S., Li, L., Lam, K.Y. and Jia, L. (2009) 'SAODV: a MANET routing protocol that can withstand black hole attack', *2009 International Conference on Computational Intelligence and Security*, 11 December, IEEE, Vol. 2, pp.421–425.
- Mahore, H., Agrawal, R. and Gupta, R. (2018) 'Agent based black hole detection technique in aodv routing protocol', *International Conference on Advanced Computation and Telecommunication (ICACAT)*, IEEE, pp.1–6.
- Mary Anita, E. and Vasudevan, V. (2009) 'Prevention of black hole attack in multicast routing protocols for mobile ad-hoc networks using a self-organized public key infrastructure', *Information Security Journal: A Global Perspective*, Vol. 18, No. 5, pp.248–256.
- Mistry, N., Jinwala, D. and Zaveri, M. (2009) 'Mosaodv: Solution to secure aodv against blackhole attack', *(IJCNS) International Journal of Computer and Network Security*, Vol. 1, No. 3, pp.42–45.
- Mohanapriya, M. and Santhosh, R. (2021) *WITHDRAWN: Detection and Elimination of Black Hole Attacks in Mobile Ad Hoc Networks*.
- Moudni, H., Er-rouidi, M., Mouncif, H. and El Hadadi, B. (2019) 'Black hole attack detection using fuzzy based intrusion detection systems in manet', *Procedia Computer Science*, Vol. 151, pp.1176–1181.
- Naveena, S., Senthilkumar, C. and Manikandan, T. (2020) 'Analysis and countermeasures of black-hole attack in MANET by employing trust-based routing', *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, pp.1222–1227.

## Bibliography

- Choudhury, D.R., Ragha, L. and Marathe, N. (2015) 'Implementing and improving the performance of aodv by receive reply method and securing it from black hole attack', *Procedia Computer Science*, Vol. 45, pp.564–570.

- Rajendran, N., Jawahar, P. and Priyadarshini, R. (2019) 'Cross centric intrusion detection system for secure routing over black hole attacks in manets', *Computer Communications*, Vol. 148, pp.129–135.
- Sandhya Venu, V. and Avula, D. (2018) 'Invincible aodv to detect black hole and gray hole attacks in mobile ad hoc networks', *International Journal of Communication Systems*, Vol. 31, No. 6, p.e3518.
- Tamilselvan, L. and Sankaranarayanan, V. (2008) 'Prevention of cooperative black hole attack in manet', *J. Networks*, Vol. 3, No. 5, pp.13–20.
- Tiruvakadu, D.S.K. and Pallapa, V. (2018) 'Honeypot based blackhole attack confirmation in a manet', *International Journal of Wireless Information Networks*, Vol. 25, No. 4, pp.434–448.
- Vatambeti, R., Supriya, K.S. and Sanshi, S. (2007) 'Identifying and detecting black hole and gray hole attack in manet using gray wolf optimization', *International Journal of Communication Systems*, Vol. 33, No. 18, p.e4610.