Int. J. of Comp. & Info. Tech., (2017) 5(3): 139-152.

IJOCIT

ISBN: 2345-3877
www.ijocit.org
Volume 5, Issue 3

*Original Research*

# Attack Detection in Mobile Ad Hoc Networks Using SVM Algorithm

**Mona Mohammad Zadeh** [1]
**Abbas Mirzaei Somarin** [2,*]

Received: 16 Apr 2017
Accepted: 30 Jul 2017



**Abstract**
Mobile ad hoc networks (MANET) as a new generation of computer networks have been designed to meet a range of specific needs. The nature of this network is open and without infrastructure that are used the magnetic waves to transfer data, and a path between nodes has no fixed router such as a switch. Generally, given the opened nature of these networks are susceptible to the influence of foreign factors more than wired networks that it's threatens the security and integrity of data in the network. On the other hand, since the nodes have no fixed resources for energy and their energy are limited, the full-time monitoring the behavior of nodes in the wireless ad hoc networks by supervisor nodes, is practically impossible. So, the importance of methods can predict attacks on the network, the more necessary. For this reason in this study an approach is presented to predict black holes and gray attacks on the network by the SVM classifier. This approach by node behavior information over a period in network, predicts malicious nodes and possible attacks of the network. The former methods continued to monitor the network and record information in the network tables, which, in addition to the loss of energy of the wireless sensor nodes, also imposed memory costs on the network. In the proposed method, there is no need to continuously monitor the nodes in the network and record the information in the table. In this approach, the source node after finding the shortest and the second shortest path to the destination in the network, sends packets Experimental and collects the data of the behavior of each node in the transmission of packets to the destination. These data are indicative of the behavior of nodes in the network that this research is based on the behavioral characteristics to distinguish abuse nodes and safe nodes and to provide a model to predict attacks. Simulation results show that the proposed method has high accuracy in classification and prediction abuse and safe nodes in the network. The accuracy of proposed method is about 95% that are comparable with previous methods in forecasting the influence of malicious nodes in the network.

**Keywords:** MANET, Network Layer Attack. Blackhole Attack, Gray Attack, SVM.

Citation: Mohammad Zadeh, M., Mirzaei Somarin, A., (2017). Attack Detection in Mobile Ad Hoc Networks Using SVM Algorithm, *Int. J. of Comp. & Info. Tech. (IJOCIT)*, 5(3): 139-152.

[1] Department of Computer Engineering, Ardabil Science and Research Branch, Islamic Azad University, Ardabil, Iran
[2] Department of Computer Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran
[*] Corresponding Author: a.mirzaei@iauardabil.ac.ir

## 1. Introduction

Mobile ad hoc networks (MANET), as a new generation of computer networks, were designed to meet a range of specific needs. The nature of network is open without infrastructure and for information transition use magnetic waves. In MANET, route between nodes hasn't fixed router such as router or switch, so it has many applications and therefore has a high popularity among business users. Each node, in addition to a final system, can act as a router and the relationship between two nodes may be connected through a several steps to each other. Despite the popularity among users exposed too many attacks, wireless links in this type of network, making them more vulnerable to attacks and attackers easily penetrate into the network and disrupt communications access. Thus the security against any threats is essential. The attacks and malicious nodes in the network cause great and irreparable damage to network. Hence, this study examined a variety of attacks in MANET and will review prevention methods of black hole attack [1].

Mobile ad hoc networks hasn't infrastructure that have been formed by a set of mobile hosts and are connected to each other through wireless links. Each node can act as a final system. In addition it can send packets as a router. In Mobile ad hoc network, two nodes may be connected to each other by a step or multiple steps. When a source node is planning to carry out data to a destination node, packets transmitted between the central nodes and so the searching and quickly creating a path from the source to the destination node is critical for mobile ad hoc networks. Mobile ad hoc networks topology may be changed periodically and displace nodes. With this technology, nodes can be easily changed with local neighbors. Devices used in mobile ad hoc networks may be present in various forms, but they have the same footprint, that means that all nodes are at least equally independent [2].

Since mobile ad hoc networks are without infrastructure and use any equipment such as routers and switches for routing, abuse and malicious nodes is inevitable. Malicious nodes can easily penetrate through other network nodes and participate in the routing operation and distort submitted information under threat. In this type of network, attack can destroy network. The security and prevention of attacks on mobile ad hoc networks has become a major challenge. Researchers have been proposed plenty of ways to detect attacks and provide security in mobile ad hoc networks [3]. Attacks in this kind of network are in network layer, in the following are some of the attacks we examined separately for each layer [4].

Mobile case networks are quickly launched due to the lack of infrastructure, so they have many applications and have therefore gained great popularity among users. But they are subject to many attacks [5]. Wireless links in these types of networks have become more vulnerable to attacks, and attackers easily penetrate the network and disrupt access to communications. Therefore, the need to maintain security against any further threats is evident. The existence of malicious nodes and attacks in network entails large and irreparable damage to the network. By predicting and detecting malicious nodes in these types of networks, it is possible to prevent the transmission of data to these nodes and to avoid hazards [4].

Hence, in this paper, we try to use the SVM method to classify unsafe and well-forwarded packets and ultimately to detect attacks. Since we have used classification methods to detect attacks, we suspect that the use of the SVM method is useful for detecting black holes and even gray attacks. The SVM algorithm is a binary classifier (two classes) that creates a boundary between available data in the two classes, which can be separated by this margin of data in the two classes. Here, our classes are healthy nodes and malicious nodes. By categorizing, the data that is located on this boundary border is classified as blocks whose number of packages has fallen. Therefore, it can be understood that the node before the node that sent the message can be a malicious node and can be detected as a gray attack.

In the rest of this article, MANET layer attacks of network are in section 2.1 available attacks on MANET transfer layer are reviewed in section 2.2. Available attacks in MANET application layer are reviewed in Section 2.3. The conclusion of the review attacks is presented 2.4. In the next of this paper, first we have review on related work of mobile Ad Hoc in section 3. The proposed method for detecting attacks in MANET is presented in Section 4. Implementation and testing of the proposed model have been done in Section 5. The conclusion and future work of this article is provided in section 6.

## 2. Survey of Attacks in Mobile Ad Hoc Network

### 2.1. The Attacks of Network Layer

WSN In performance, in classification of each layer of the OSI model, network layer selecting the appropriate route and is responsible to deliver packages properly. These layers can divide functions in two main parts: Packet forwarding and routing. . As it is clear, the designing of the layer is depended totally to ad hoc structure. Attack in mobile network can be performed in both main parts of the network layer. In practice, security in routing and prevention of attack risks such as identification designed based on resource availability, integrity, confidentiality and privacy. In Packet forwarding, a node can be in attack of any unconventional action, such as package sending, changing the package content, disturbing sequence of packets at the network layer [5].

*2.1.1. Black Hole Attack*

In the black hole attack, a malicious node using routing protocols in the destination direction of the node. As the shortest route, remove packets in the destination node; this malicious node by sending fake messages introduced himself as the shortest route. As a result, the source node regardless to routing table selects route method. In this method, malicious node is always available to respond to the source node and thus the source node passes packets through this route and the malicious node start to remove packets [6].

In this protocol, when the request message of route is sent, malicious nodes receive response before real nodes and response quickly, hence create destructive path and when the route was created, it doesn't check that the node is malicious or not. All packages are sent via this unknown address. The way how malicious nodes are in routes, is shown in figure 1. A malicious node Z listens when a legal node A requests route to another node, the C', Node Z has this data and claims this is the shortest route to reach C. As a result, A sends package to Z and is expected to reach packets to C, but Z don't send packets to C. The consequences are that nodes aren't connected to the rest of the network.


**Figure 1:** Examples of black hole attack [6]

This attack is special attack of black hole that attacker node remove groups of packages optionally after absorbing partially and will send rest .In this attack, the attacker node is one of the central nodes farther away from the source node and take part in routing and send the RREQ packets to the destination node and send RREP packet to the source node. But in the process of information exchange, try to prevent some information arrival. For example, only 60 percent of the information sends from the source node to the destination node and it keep rest information. Attack of gray node has fewer risks to the network but invasive identification process is more difficult than attack of black hole. The attackers node is a type of Spyware in gray node attack .In new ways of these attacks, the attacker node by RERR package reports to source that internal node interrupted connection with network or has a farther distance than and thus try to destroy the other nodes and source node finds more complex and more reliable situation to communicate with attacker node. Figure 2 shows the characteristics of black holes attack.

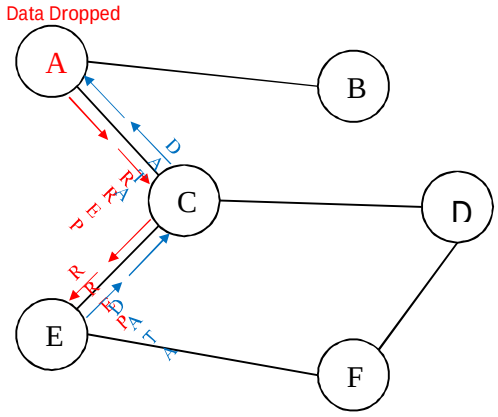


**Figure 2:** The properties of the black hole attack

- **Black Hole Attack in DSR Protocol**

Many possible reasons abuse the network, including faulty software or hardware. Classic wired networks run by operator who select equipment as fault on the network; this means that an important source is not available. In wireless ad hoc networks where equipment provided by user, expected that this kind of problem does not exist. Some nodes may participate by modifying route in the routing. But packets get healthy through this route. Another reason for this type of network attacks is their desire

to save more battery power. Finally, some of the nodes may be a malicious node and try to create weakness in the network, such as viruses, wormholes, black holes. If a bad behavior of node is identified by neighbors, neighbors can withdraw to provide services in these nodes. Thus causing the normal routing nodes, this will result in resource savings. Otherwise harm occurs in the network performance and healthy nodes do not participate in routing to create a healthy path [7].

- **Black Hole Attack in the AODV Protocol**

There are two types of black hole attack in AODV routing protocol:

Attack of internal black hole made by malicious nodes placed between destination nodes and passes this route as soon as the packet arrived. The chance of this type of nodes is more and nodes are able to attack at this stage, it is a kind of black hole attack that owned itself to data path. This type of attack is difficult to detect.

The outside attack of black hole is physically outside of the network. Attack of black hole can be converted to inside attack, when malicious nodes control the internal and external malicious nodes of MANET networks. Foreign malicious nodes can be summarized into the following sections [8]:

- The malicious nodes are always active in routing and locate itself in the path of destination nodes.
- Malicious nodes always with false RREP messages want to be on the path of destination node. With a lower number of steps try to forge a path.
- The black hole nodes by sending RREP to its nearest neighbors, as the active path, are trying to access the source node. And also the source node uses this route as a healthy way.
- When new information obtains from the call path, allow the source node to update its routing table.
- The new route is selected by the source node to send data.
- All nodes start to remove malicious packets that sent from this path.

In AODV routing protocol, attacks happen when (A) malicious node identifies (E) sender and destination node of (D) in the active path. Start sending fake RREP with lower step than normal number toward C node, C sends RREP to sender E node; and finally the path is the malicious node and these packages will be removed by malicious nodes [9].

*2.1.2. Attacks of Gray Nodes*

For example, by forging a routing message, an attack intended to scramble for routing, intercepting, removing packages and threaten safety features that mentioned above. Black holes attack is common in mobile ad hoc networks and prevention of the attack is a crucial point in mobile ad hoc networks. Attack takes place by a node or several nodes [4].

The attack is special gray node attack and attacker node after absorbing the packages of node put away a group, and sends others. In the attack, attacker node is the central nodes or a node away from the source node and takes part in the routing and send packet RREQ to the destination node and also send RREP packet from the destination node to the source node, but during the exchange of information, it tries to prevent arriving some information. For example, only 6% of the information leads from the source node to the destination node and keep the information to itself. Gray- hole attack has fewer risks for network but node identification process is more difficult than the black hole attack. In fact, the attacker nodes in gray hole attack is a type of Spyware and behaves in a way that two nodes are not suspicious and exchange essential information between them. In New methods of the attacks, the attacker node by RERR reports to source node that the network connection is interrupted or is in a farther distance than it, and thus try to destroy the other nodes and the situation is more complex and source node finds more reliable and complex situation to communicate with the attacker nodes [10].

*2.1.3. Wormhole Attack*

The very famous attack of ad hoc networks is the wormhole. In this attack, hostile provide a short link in the topology of network. The attack is executed as follows. A routing request from one node sends to the hostile nodes, this hostile node sends the request through a private network to the second node. Now, if these two nodes, the hop counters, do not change directions, much of the route is traveled by private network without increasing the amount of hop. So depending on the destination, instead of ten hops; only two hops will arrive. In this case, surely a route is selected as the shortest route [11]. Figure 3 shows an example of the attacks.

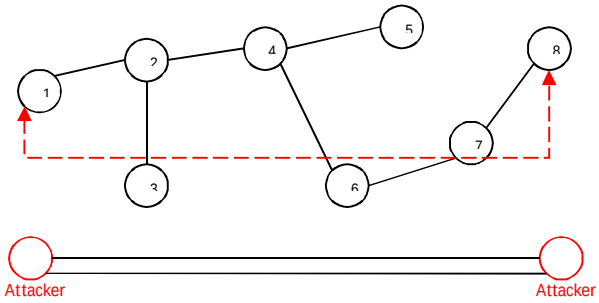


**Figure 3:** An example of wormhole attacks [11]

*2.1.4. Rushing Attack*

In the active attack, two hostile nodes use tunnel process for the wormhole. If the rapid transmission of path exists at both ends of the communication channel, internal packets of tunnel release faster than normal routes. This type of attack is Rushing that can be used as a kind of service denial on reactive routing protocols of mobile ad hoc networks.

**2.2. Transport Layer Attacks**

The main objectives of the transport layer protocol in mobile ad hoc networks are: step by step linking, step by step reliable delivering of packets, flow control, and congestion control. As TCP protocol of Internet, mobile nodes are more vulnerable in SYN flooding or hijacking attacks.

*2.2.1. Torrential Attacks*

This type of attack is denial of service. The attacker exploits weakness of TCP / IP protocol. Layer of TCP protocol uses SYN and SYN / acknowledgement (ACK) to establish a connection. Action is expected to the host sends a SYN packet and waits to receive SYN / ACK packet from the receiver. With The SYN attack, the attacker simply sends SYN packets, and thus causes failure of the network.

*2.2.2. Hijacking Attacks of a Meeting*

Eavesdropping attacks on the network means eavesdropping and removal of packets in order to transfer to the destination. This type of attack occurs when a protocol session, TCP / IP, to be removed by a participant. This means that the transmission of a message between sender and receiver, changes in posture of message and a revised message flow on the network traffic again. With these changes, penetrating message is defined as the destination. All future messages defined in the meeting (session) will be between origin and penetrating (as a new destination) and traffic redirects to the desired destination of attacker, all incoming packets go toward the attacker [12].

**2.3. The Attacks of Application Layer**

In this layer, attacks can be divided into two categories: virus attacks and worm attacks.

*2.3.1. Virus Attacks*

Methods of spreading the virus, which is located in the boot sector which virus is active in start time. There are a variety of methods for virus replication in the network. Virus replication requires a host application that is installed in the host computer and through the program starts its activity. A virus does not infect data files, because the files are not running and are not part of the executive that helps to virus. Sometimes viruses are transmitted in encrypted form on the network. The purpose of the virus coding, is not to create privacy for data, but the aim is to change the shape of the virus in order to network is not detected by security tools like firewall or IDS and decoded and implemented in their destination. According to a HOST program and is published based on the excitatory that may respond to the user (such as clicking by the user). Sometimes irrelevant programs giving the message to the user and choose one of the YES / NO buttons so that they allowed to be installed and we are unaware that both YES / NO options are same and user by No option give positive response to attack [13].

*2.3.2. Worm Attacks*

In addition to the viruses that are active in a network application layer, there are worms. Worms spread automatically and do not need to stimulate through user's side. The performance of worms is independent and does not need host application [14].

**2.4. Comparing the MANET Attacks and Conclusions**

Different attacks of OSI model reviewed in the previous study. In this section we will compare MANET attacks. Table 1 shows General description of attacks and function of network.

**Table 1:** Comparing MANET attacks

| Attack | Performance on The Network | The Number of Nodes | Layer |
|---|---|---|---|
| Black hole | Insertion as fake nodes and removing of packages | One or more | Network |
| Gray | Insertion as fake nodes and removal part of the package | One or more | Network |
| Hole worm | Create a false path and exiting multi-node of the way and change in packaging | At least two | Network |
| Rushing | collusion of nodes and creating a tunnel for quick transfers and denial of service | At least two | Network |
| Flooding | sending SYN , not ACK packets and network disruption | One or more | Transmission |
| Hijacking of a meeting | Forging or changing transited message destination and re-insert the modified message in the network traffic flow | One or more | Transmission |
| Virus | Malicious resident programs on the host, replication by stimulating specific application and infecting of data | - | Application |
| Worm | Such as virus with automatic replication | - | Application |

This paper presents a brief review of mobile networks and different types of attacks at the different network layer. Mobile networks are without infrastructure thus this type of network is more vulnerable to attack than other networks. So you need to reviews more accurate these types of attacks in mobile ad hoc networks that to ensure mobile networks can be used more.

Since in ad hoc mobile networks, nodes are not connected to a stable energy sources to attain power and can provide the required energy from batteries with limited energy, thus complete control by observer leading to the rapid completion of the nodes energy and may interfere in the network communications. The approaches, that are not permanent performance monitoring of network nodes and classification of nodes takes place based on behavioral characteristics of the nodes, appear to be effective ways to detect attacks on wireless networks.

## 3. Background of Mobile Ad Hoc Attacks

In the black hole attack, a malicious node using routing protocols in the destination direction of the node. As the shortest route, remove packets in the destination node; this malicious node by sending fake messages introduced himself as the shortest route .As a result, the source node regardless to routing table select route method. In this method, malicious node is always available to respond to the source node and thus the source node passes packets through this route and the malicious node start to remove packets [15].

Latha et al. [16] have proposed a solution to enhance the efficiency of the AODV routing protocol, which will be able to detect and prevent some of the black holes that act as a group. This method uses a correct table to combat with black hole attack, so that each participant node is assigned a correct level, which is a unit of measurement for the reliability of a node. In this case, the level of each node that is removed is set to zero in the table and that malicious node considers as the black hole and deleted.

Medadian et al. [6] presented a method that uses a number of rules to ensure that sender's response is honest. Activities of a node are recorded by its neighbors. These neighbors ask other nodes to submit their comments about this node. When a node aggregates the views of all its neighbors, that node decides if the respondent is a malicious node, the decision is based on the number of rules. Judging is based on activity of nodes in the network.

Xin Li and colleagues [17] presented a reliable packet-based model, measuring the PFR in a node based on the ratio of the number of packets sent to a number of packet information. PFR assigns a reliable coefficient to each node. If a node operates correctly in routing and sends packets to the destination, then increases the reliable coefficient of this node, otherwise the decreases trust coefficient of that node.

Kumar et al. [18] have proposed a more effective solution to detect black hole attack with lower-cost in MANET, which is less vulnerable to mobility and subscription-based nature compared to infrastructure-based networks [18]. In this method, when a source node (S) wants to communicate with the destination node (D), the source node sends the routing request (RREQ) to the entire network. Then all input routing responses are aggregated into a table called Current Routing Response Table (CRRT). The routing response will be collected until the expiry date of the RREP packet expires. The source node (S) must define the threshold (TH) used to confirm the order number of the routing response time in the selected node. If the order number (arrival time of the routing response) is greater than or equal to the threshold value, then that path is treated as a path with a black hole node. Otherwise, that path is a healthy node, and it is used to communicate with the destination node based on the destination sequence number.

Patil et al. [19] have proposed a new approach to prevent black hole attack in DSR based on path storage. In this method, after the black hole node has been identified in the MANET during the path construction, the black hole ID is sent to the DSR routing function. In this function, the paths are ready to be added to the path cache; however, the priority of adding each path in the path cache is determined by the presence of the identifier of the black hole node in the path of decision. If it looks like black hole, it simply removes this path and adds all the other paths that are considered for the source in the two-way communication of the destination, to the path cache. This process uses only the process of path storing in a natural time.

Kshirsagar et al. [20] have provided a method for detecting and preventing a black hole attack in real time by monitoring the suspicious nodes by their neighboring nodes. When a source node wants to transfer some data, it will diffuse the RREQ request packet. As soon as a middle node receives this packet, it checks whether it is a destination path or not. If it has a destination path, the middle node generates a Routing Response Packet (RREP) and sends it to the source node; otherwise it sends the middle node of the RREQ packet to its neighbor node. When a middle node (the suspect node) receives a RREQ packet, it generates a RREP packet and sends it to a source node in a single-sided manner. In this method, the neighboring node of the RREP sender node is identified first (for example, a suspected node) and the neighboring node is ordered to eavesdrop / listen to all packets sent by the suspect node. For eavesdropping packets sent by a suspicious node, neighbor's node places itself in the irregular state.

## 4. Proposed Method

In order to detect black hole attacks, in the first stage, the source node sends the routing request (RREQ) to the network and waits to receive the RREP request response. Of course, the first response to a routing request (RREP) is the shortest route to the destination node. After determining the shortest path, the source node waits for another RREP request to find another route to the destination. This next route is actually the second shortest route to the destination. It should be noted that the shortest path is the most probable route for the presence of malicious nodes (s) .To find out, it's just time to compare the number of steps in the shortest and second shortest paths. If the difference between the length and the time of receive response is abnormally high on these two routes and this value is greater than a user-specified threshold, the closest path is suspicious and probably exist malicious nodes (s) in this path.

Currently, the source node sends a portion of packets that have a specified volume through each of the closest and second closest routes and waits for the ACK message of each node. Before sending blocks, the source node counts the volume of sent packets and then sends packets. Along the way, each node that receive the information sends an ACK message, which includes the number of packets and the number of the former nodes from which packets are received, and send it to the source node. This message is sent by all the nodes in both directions. Eventually, after destination node received the data blocks, it sends an ACK message to the source node via the same route as the packets received. The source node reviews the classification of nodes by

receiving these messages from the SVM algorithm [21, 22, 23]. An example of routing and ACKs receiving is shown in figure 4 [15].

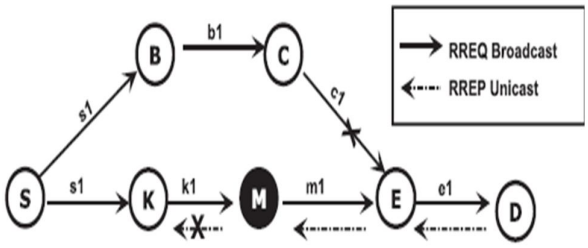


**Figure 4:** An example of routing and ACK receiving in the proposed method [15]

For example, let's assume that the s node starts to rotate as the source node. In this case, the node starts to broadcast RREQ and then waits for RREP .RREQ is transmitted in the two paths indicated in Figure 1 as s1, b1, c1, e1, and in the second path, S1, k1, m1, e1, respectively. After the RREQ arrives to the destination node D, the RREP routing request response is propagated through the D→E→C→B→S and D→E→M→K→S nodes in both directions.

Given these paths, the source node begins to send packets. Each node that receives the packet sends the ACK on the path to its predecessor, and the ACK is sent along the path to the source node, respectively. If the source node does not receive an ACK node from a RREP path, then assume that before this node, our node is a malicious and depending on the volume of packages, we begin to classify the nodes.

The important thing to note here is that if a node moves along a path and ACK is not received from it, the previous node is also mistakenly considered as a malicious node, while the malicious node is not a malicious node that threatens the accuracy of the proposed method. So, in the scenario of the proposed method, we should consider the minimum movement for the nodes.

The SVM class divides the nodes of the network into -1 and +1 classes. Then, depending on the behavior of the nodes, they assign them to the classes and specify the boundary between the two classes. Naturally, one of the features that the SVM classifier will use to decide is the packet size reached by each node during the test packet submission. Other features of the nodes include the transmission protocol, the length of the connection path, the traffic information like number of communication paths, the number of sent packets, the number of lost packets, and so on. If the package reached to the node of the path must not be sent to the node before it is sent to the path at all, this node is located as a node in class -1, and the type of attack, is predicted the black hole attack. Also, if the volume of packets reached in the path is complete and the difference is very small, the node in the path is classified as a healthy node in the class +1. The third mode is when the volume of the reached packets is between the two classes and the borderline; In this case, the nodes of these packets in the path will be as malicious nodes and attack type. The flowchart of proposed method is shown in figure 5.

## 5. Implement of Proposed Method

In this subsection, in order to implement the proposed method, we first simulate the mobile network in the presence of malicious nodes, and we will extract the necessary information about the number and volume of packets sent by nodes in the path of this network. Then, by these data, we will classify and predict malicious nodes by the SVM class according to the node behavior in the network.

First, a black hole attack scenario in the network was simulated with the presence of malicious nodes in the mobile network by the NS-2 network simulator. And with attention to scenario parameters, proposed mobile network is implemented in table 2.

**Table 2:** Proposed MANET parameters

| Parameters | Amount |
|---|---|
| Channel type | Wireless |
| Channel standard protocol | Mac/802_11 |
| Maximum queue size | 50 packet |
| Maximum packet size | 1020 byte |
| Number of nodes | 28 node |
| Transfer protocol | AODV |
| Simulation environment | 1000*1000 |
| Simulation time | 35 seconds |

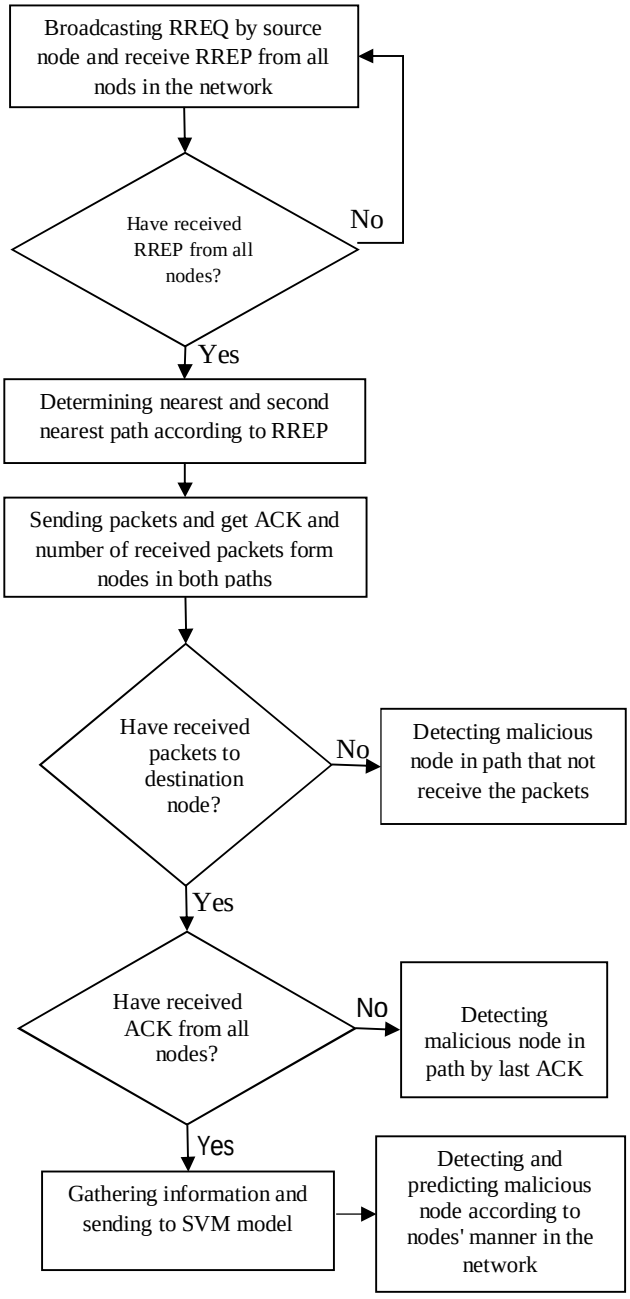


**Figure 5:** Flowchart of proposed method

## 5. Implement of Proposed Method

In this subsection, in order to implement the proposed method, we first simulate the mobile network in the presence of malicious nodes, and we will extract the necessary information about the number and volume of packets sent by nodes in the path of this network. Then, by these data, we will classify and predict malicious nodes by the SVM class according to the node behavior in the network.

First, a black hole attack scenario in the network was simulated with the presence of malicious nodes in the mobile network by the NS-2 network simulator. And with attention to scenario parameters, proposed mobile network is implemented in table 3.

**Table 3:** Proposed MANET parameters

| Parameters | Amount |
|---|---|
| Channel type | Wireless |
| Channel standard protocol | Mac/802_11 |
| Maximum queue size | 50 packet |
| Maximum packet size | 1020 byte |
| Number of nodes | 28 node |
| Transfer protocol | AODV |
| Simulation environment | 1000*1000 |
| Simulation time | 35 seconds |

According to the proposed method, the source node initially diffuses the request throughout the network. The nodes on the network send the response to the source node by receiving a routing request. All existing nodes send the routing response in the form of the ACK message to the source node, and the source node, after receiving routing responses, attempts to identify the shortest path and the second shortest path. In the present scenario, the shortest route consists of {26-3-7-21-2-6} nodes and the second shortest path consists of {26-8-25-15-5-2-6} nodes.

The source node, after identifying the nodes in the shortest and second shortest paths, sends packets through the nodes to the destination node. As expected, the shortest route has a malicious node, which puts itself as the destination node. This malicious node is the number 3 node that receives and destroys packets from node 7 that are located in the path of source to this node. After the source node has transmitted the packets through the shortest path, it is time to send the source node of the packets via the second shortest path according to the proposed method. The source node sends information packets in the path of the shortest path, and stores ACK messages from all path nodes.

As noted, the information needed to retrieve the trace file from the simulation of the scenario includes the number of the participant node in communication, the sent/ received packet size, and the number of packets that each of the nodes received on the route .They are an example of the retrieved information in table 4. Also, according to the extracted information from the simulation scenario, table 5 shows the characteristics of nodes in the network about the number and volume of sent, received, deleted, and lost packets. These features will serve as a benchmark for deciding the behavior of nodes in the network by the SVM classifier.

### 5.1. Implementation of SVM Classification

As noted, the SVM classification is one of the most widely used methods among data mining techniques. This two-class classifier uses the data attribute and specifies the distinction between classes, and tries to maximize the distance between the classes in terms of the data characteristics in the classes. In this paper, our classes are healthy and malicious nodes in the case network, and their features derived from network simulation include the number and volume of sent, received, and lost packets. And the number and volume of feedbacks sent by all the nodes in the network. The SVM classification deals with modeling with regard to the features of the nodes in the selected path. Given that the network nodes in the grid are marked from the beginning, the class label of the nodes is clearly identified on the network. The SVM class identifies the malicious nodes in the network by these class properties and labels .These nodes are identified with respect to their abnormal behavior relative to other nodes and based on specified characteristics.

**Table 4:** An example of the retrieved information from *trace* file

| Event | time | node | protocol | Packet size | Source address | Destination address | sequence num | Packet id | Packet type |
|---|---|---|---|---|---|---|---|---|---|
| s | 3.757518781 | 9 | AODV | 48 | 9:255 | -1:255 | [26 7] | [6 8] | Request |
| r | 3.757963021 | 25 | AODV | 48 | 26:255 | 6:255 | [26 7] | [6 8] | Reply |
| f | 3.752052096 | 8 | AODV | 44 | 26:255 | 6:255 | 0x4 | [26 8] | Reply |
| D | 1.269853906 | 3 | cbr | 1020 | 6:0 | 26:0 | [27 3] | [3] | - |

**Table 5:** Extracted information of the simulation scenario

| Node number | Number of received packages | Volume of received packages | Number of sent messages | Volume of sent messages | Number of feedback packages | Volume of feedback packages | Number of lost packages | Volume of lost packages |
|---|---|---|---|---|---|---|---|---|
| 1 | 193 | 159824 | 4 | 192 | 156 | 158144 | 0 | 0 |
| 2 | 112 | 86024 | 8 | 320 | 85 | 83772 | 3 | 144 |
| 3 | 50 | 32524 | 4 | 192 | 33 | 88 | 121 | 1265 |
| 4 | 82 | 50508 | 4 | 192 | 49 | 49004 | 0 | 0 |
| 5 | 41 | 1872 | 4 | 192 | 35 | 1624 | 3 | 144 |
| 6 | 262 | 239072 | 480 | 480952 | 0 | 0 | 0 | 0 |
| 7 | 65 | 34200 | 5 | 224 | 34 | 32728 | 1 | 1020 |
| 8 | 68 | 49904 | 4 | 192 | 52 | 49136 | 0 | 0 |
| 10 | 191 | 159744 | 4 | 192 | 15 | 44 | 417 | 2015 |
| 15 | 77 | 50312 | 4 | 192 | 50 | 49048 | 0 | 0 |
| 21 | 66 | 30300 | 5 | 224 | 39 | 28604 | 0 | 0 |
| 25 | 83 | 50616 | 4 | 192 | 50 | 49048 | 0 | 0 |
| 26 | 245 | 237392 | 192 | 188176 | 0 | 0 | 0 | 0 |

After identifying malicious nodes in the network and classifying them in a separate class, the boundary between the two classes is determined. The boundary is between the two linear classes that separates the two classes. In addition to the separator line between the two classes, the SVM classifies the margin for separation of the two classes. This margin is, in fact, the threshold for specimens to fall into classes, and naturally the threshold is the same for both classes. If discussed formally, the distance between the boundary line and the upper border, that is the upper class separator or +1, is equal to the distance between the lower boundary line with the lower class separator or -1. Examples that have higher specification values than the upper boundary line are definitely the upper class or +1. In this paper, Class +1 represents the healthy nodes in the network. Also, samples that have lower attribute values than the lower boundary line are definitely in the lower or lower class. In this paper, class -1 represents malicious nodes in the network. Examples that are distributed in the space between the boundary line and the border line cannot be definitely decided on their class. These samples are close to the decision boundary and may be part of another class that is mistakenly sorted. In this research, such examples are considered as nodes to malicious nodes with gray attacks. The classification of the existing nodes proposed by the SVM classification is shown in figure 6.

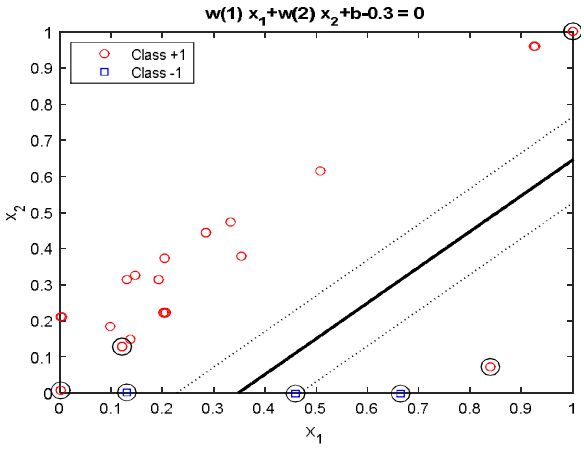


**Figure 6:** Classification of nodes in proposed scenario

.

### 5. 2. Performance Evaluation of Proposed Method

According to figure 7, the error in the classification of the SVM classifier is the distance from a data point of the+1+ (1-) class in the 1 + (1) class separating line, If this data point is mistakenly classified in the data points of 1 (+1) Class. The total of these errors is considered as a general error of the classification model and the average of these errors is considered as the average error of the classifier model for the total data. The nodes that do not apply in these conditions have a zero error value, which means that these nodes are properly categorized. Figure 7 (a, b) shows, respectively, the diagram of the errors in the train and test phase of the proposed model on the nodes in the connection path according to the proposed scenario.

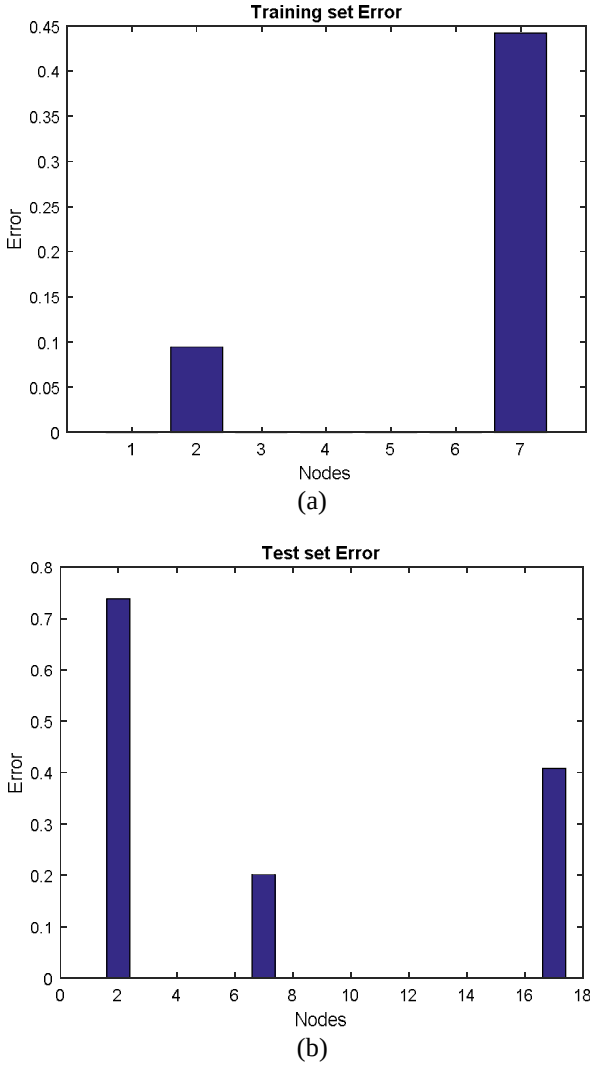


**Figure 7:** Errors diagram in the train and test phase of the proposed model

As can be seen in Figure 4, the nodes that are properly classified have a value with zero error and the nodes that have errors with value greater than zero. Existing errors are considered as system weaknesses, while the well-classified nodes are considered as the strengths of the proposed model and are considered as the precision of the proposed method. Figure 8 (a, b) shows, respectively, the accuracy diagram of the proposed method in the train and test phase on the nodes in the connection path according to the scenario.

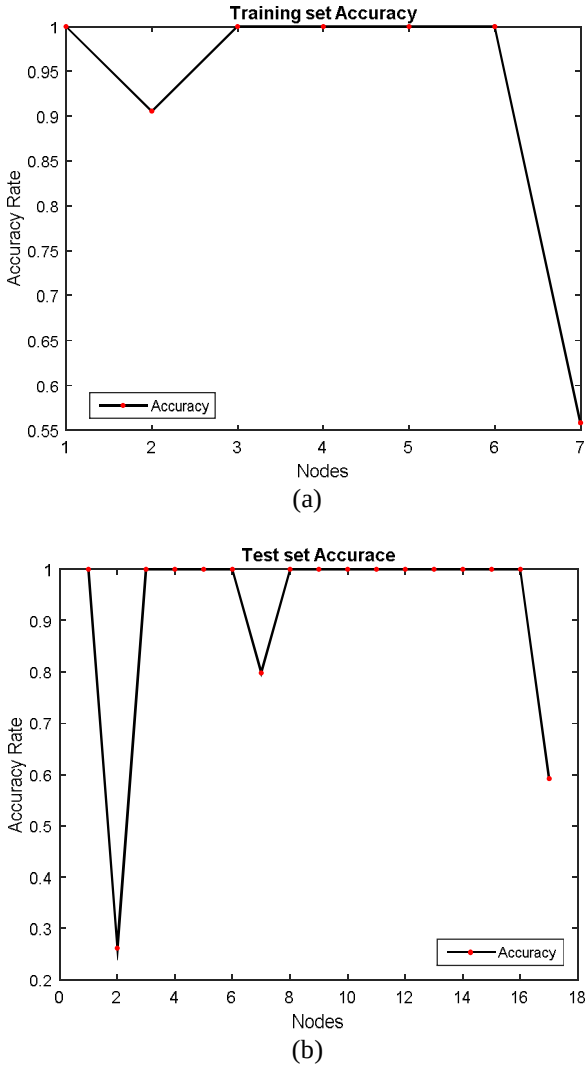


**Figure 8:** Accuracy diagram in the train and test phase of the proposed model

As can be seen in figure 8, classification accuracy for well-classified nodes is equal to one and classification accuracy for nodes not properly classified is less than one. Figure 5 provides the accuracy of the proposed method for each nodes of the path, provided that the average accuracy for the proposed method is obtained of the average accuracy

of all nodes. Therefore, in order to obtain the accuracy of the proposed method on the training nodes in the path specified in the proposed scenario, we obtain the average accuracy of the nodes. In this paper, the average accuracy of the proposed method for all nodes in the network is 94.61%.

### 5.3. Comparison of the Proposed Method with Previous Methods

Comparison of the proposed method with previous methods is done to predict malicious nodes in order to measure the validity of the proposed method. The comparison of the proposed method with [22, 23, 24, 25, 26, 27] is shown in figure 9.

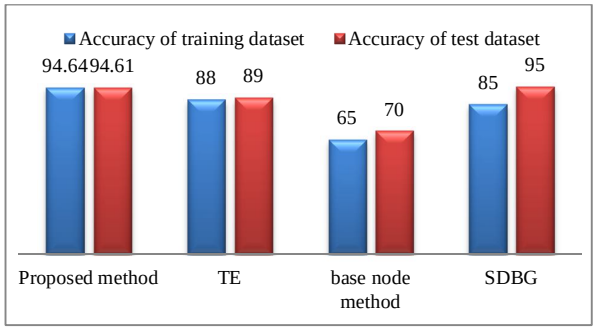


**Figure 9:** Comparison of the proposed method with prior works

As shown in Figure 6, the proposed method has a good accuracy in predicting malicious nodes of mobile case network and is comparable with previous methods in predicting malicious nodes and network intrusions.

## 6. Conclusions and Future Work

In this paper, a method for learning a machine based on the SVM classifier is proposed to detect the prediction of malicious nodes and attack to MANET and take into account node characteristics in the network. By detecting healthy and destructive nodes, it is possible to predict the attacks on the path. Hence, with the prediction of attacks on the route, there could be a safe route and a safe route. The simulation results show that the proposed method has high accuracy in classifying and predicting harmful and harmful nodes in the network. The precision of the proposed method is about 95%, which is comparable with previous methods in predicting malicious nodes and network infiltration.

In the future, in the field of detecting and anticipating attacks in the mobile case networks, one can combine class divisions to increase the accuracy of classification and prediction of bad nodes and, ultimately, attacks on the network. In addition, by combination of probabilistic functions with class divisions can be another improvement on this article, which allows you to examine and predict new and unknown types of attacks.

## References

[1] Lu S, Li L, Lam K, (2009), "SAODV: a MANET routing protocol that can withstand black hole attack", Computational Intelligence and Security. International Conference, pp: 421-425.

[2] Shanthi N, Ganesan L, (2009), "Study of different attacks on multicast mobile ad hoc network", Journal of Theoretical & Applied Information Technology, pp: 6-12.

[3] Mahajan V, Natu M, Sethi A, (2008), "Analysis of wormhole intrusion attacks in MANETS", Military Communications Conference, pp: 1-7.

[4] Biswas K, Ali M, (2007), "Security threats in mobile Ad Hoc network", Department of Interaction and System Design School of Engineering, pp: 9-26.

[5] Jani P, (2002), "Security within Ad-Hoc Networks", Seminar on Network Security Position Paper, No.200, pp: 16-17.

[6] Medadian M ,Fardad K, (2012), "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", *European Journal of Scientific Research*, pp: 91-101.

[7] Rajesh J. Nagar, Kajal S. Patel, (2012), "Securing AODV Protocol against Blackhole Attacks", *International Journal of Engineering*, p:1116-1120.

[8] Muhammad AI, Seong M, Seungjin P, (2004), "Black Hole Attack in Mobile Ad Hoc Network", *Proceedings of the 42nd annual Southeast regional conference*, pp:96-97.

[9] Jaisankar N, Saravanan R, Swamy KD, (2010), "A Novel Security Approach for Detecting Black Hole Attack in MANET", International Conference on Recent Trends in Business Administration and Information Processing, India, pp:26-27.

[10] Hesiri W, Huirong Fu, (2008), "Preventing cooperative black hole attacks in mobile ad hoc networks: simulation implementation and evaluation", *International Journal of Software Engineering and Its Applications*, pp:39-54.

[11] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh, (2011), " A survey of black hole attacks in wireless mobile ad hoc networks", *International Journal of Software Engineering*,.p:1-16.

[12] Bahuguna R, Mandoria H lal, and Tayalp I., (2013), "Routing Protocols in Mobile Ad-Hoc Network: A Review", Institute for Computer Sciences, pp:52–60.

[13] R. Kesavan, V. Thulasi Bai, (2012), "Avoidance of Black Hole Attack in Virtual Infrastructure for MANET", *International Journal of Computer Applications*, pp: 0975–8887.

[14] Tarandeep K., Amarvir S., (2013), "Performance Evaluation of MANET with Black Hole Attack Using Routing Protocols", *International Journal of Engineering*, pp:1324-1328.

[15] Mandala S, Abdullah A.H, (2013), "A Review of Blackhole Attack in Mobile Adhoc Network", International Conference on Instraumentation, Communication, Information Technology.and Biomedical Engineering, pp 339-344.
[16] Latha T, Sankaranarayanan V, (2008), "Prevention of co-operative black hole attack in MANET", *Journal of networks*, PP: 13-20.
[17] Li X, Jia Z, Zhang P, Wang H, (2010), "A Trust-based Multipath Routing Framework for Mobile Ad Hoc Networks", Seventh International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp: 773-778.
[18] Kumar V, Kumar R, (2015), "An Adaptive Approach for Detection of Black hole Attack in Mobile Ad hoc Network", International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science, vol: 48, pp: 472–479.
[19] Patil P.N, Ashish T, (2013), "Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching", IEEE, DOI: 978-1-4673-5999-3/13.
[20] Kshirsagar D, Patil A, (2013), "Blackhole Attack Detection and Prevention by Real Time Monitoring", IEEE 31661, 4th ICCCNT, Tiruchengode, India, pp 1-5.
[21] Zhang F, Zhou Q, (2014), "HHT–SVM: An online method for detecting profile injection attacks in collaborative recommender systems", *Knowledge-Based Systems*, Vol: 65, pp: 96–105.
[22] Kotu V, Deshpande B, (2015), "Predictive Analytics and Data Mining Concepts and Practice with RapidMiner", Elsevier, *Morgan Kaufmann, USA, chapter 4*.
[23] Ning T.P, Michael S, Vipin K, (2006), "Introduction to Data Mining", *Pearson Addison-Wesley, chapter 5*.
[24] Chatterjeea N, Manda K, (2013), "Detection of Blackhole Behaviour using Triangular Encryption in NS2", Procedia Technology, 1st International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA), vol:10, pp:524–529.
[25] Jain S, Khuteta A, (2015), "Detecting and Overcoming Blackhole Attack in Mobile Adhoc Network", International Conference on Green Computing and Internet of Things (ICGCIoT), pp: 225-229.
[26] Diep P.T.N, Yeo C.K, (2015), "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks", *IEEE Transactions on Mobile Computing*, DOI 10.1109/TMC.2015.2456895.
[27] Bang J.H, Cho Y.J, Kang K, (2017), "Anomaly detection of network-initiated LTE signaling traffic in wireless sensor and actuator networks based on a Hidden semi-Markov Model", *Computers & Security*, vol: 65, pp: 108-120.