







Use of Node credibility and Andrews plot to detect and prevent BHA in MANET

Ankita Kumari^{1*}, Sandip Dutta¹ and Soubhik Chakraborty²



¹Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Jharkhand, India; ²Department of Mathematics, Birla Institute of Technology, Mesra, Jharkhand, India

E-mail/Orcid Id:

AK,  ankitakmr33@gmail.com,  <https://orcid.org/0000-0002-0338-915X>; SD,  sandipdutta@bitmesra.ac.in; SC,  soubhikc@yahoo.co.in

Article History:

Received: 30th Jan., 2023

Accepted: 14th Apr., 2023

Published: 30th Apr., 2023

Keywords:

Andrew's plot, Black Hole Attack, credit-based system, credibility, security, MANET

Abstract: The MANET wireless network operates independently of any infrastructure and can establish connections dynamically, making it highly accessible regardless of the environment. However, the network is vulnerable to attacks such as the BHA, which can cause the depletion of the network. This attack introduces MNs into the network, providing false routing information to the source node. This leads to the drop of data packets and ultimately damages the network. To address this issue, we propose a node credibility-based approach that utilizes Andrew's plot to assess node credibility after several transactions. This method enables us to identify highly credible nodes which can be considered trustworthy in the network. We utilized Network Simulator software to create various MANET scenarios and test the effectiveness of our proposed approach against the BHA.

Introduction

MANET stands for Mobile Ad-hoc Network, which is a self-configuring network of mobile devices or nodes connected without the need for a fixed infrastructure or central administration. The nodes in a MANET communicate with each other by forming a network, which can be set up anywhere, anytime, and without any prior configuration. In a MANET, each node functions as a router, forwarding data packets to other nodes in the network until the packets reach their destination. The communication in a MANET can be achieved through different types of wireless technologies, such as Wi-Fi, Bluetooth, or Zigbee. The nodes can also use multiple wireless technologies simultaneously to establish a connection with other nodes in the network. The communication in a MANET can be classified into two types: unicast and multicast. In unicast, a node sends a message to a single destination node, whereas, in multicast, a node sends a message to a group of nodes. To establish a connection in a MANET, the nodes use a routing protocol that enables them to determine the most efficient path for transmitting data packets. The routing

protocols used in a MANET can be classified into two types: proactive and reactive. Proactive protocols maintain a constant routing table, whereas reactive protocols create a routing table only when needed. One of the most significant advantages of MANET is its ability to operate in a dynamic environment. The nodes in a MANET can move around freely, and the network can adapt to the changes in topology without any disruption. This feature makes MANETs suitable for applications that require mobility, such as military operations, disaster management, and vehicular communication. However, MANETs also face several challenges, such as limited bandwidth, security, and scalability. The limited bandwidth can affect the network's performance, while security concerns arise due to the absence of a central administration. The scalability of the network is also a challenge as the network's performance degrades with the increase in the number of nodes. MANETs provide a flexible and robust communication solution for applications that require mobility. However, the network's performance depends on the selection of an appropriate routing protocol, addressing scheme, and security mechanisms.



Table 1. Message format of Route Request (RREQ)

| Type | J* | R** | G*** | D**** | U***** | Reserved | Hop Count [@] |
|---|----|-----|------|-------|--------|----------|------------------------|
| RREQ ID [#] | | | | | | | |
| Destination IP Address ^{##} | | | | | | | |
| Destination Sequence Number ^{###} | | | | | | | |
| Source IP Address ^{####} | | | | | | | |
| Source Sequence Number ^{#####} | | | | | | | |
| *The letter J stands for Join Flag, which is utilized for multicast purposes. | | | | | | | |
| **The letter R represents Repair Flag, which is also used for multicast. | | | | | | | |
| ***The letter G indicates Gratuitous RREP Flag. | | | | | | | |
| ****The letter D denotes Destination Flag, which is utilized by the receiving node or the destination in the network to respond to the RREQ message. | | | | | | | |
| *****The letter U represents Unknown Sequence Number, which displays the sequence number of the destination node. The field labeled Reserved is sent as 0 and should be discarded upon reception. | | | | | | | |
| [@] Hop Count: The number of hops from the source IP address to the destination node IP address. | | | | | | | |
| [#] RREQ ID: A sequence number uniquely identifying the RREQ message and associated with the source node. | | | | | | | |
| ^{##} Destination IP Address: The IP address of the destination node that is being requested. | | | | | | | |
| ^{###} Destination Sequence Number: The sequence number of the destination node, which is updated by the last node that received the information from the destination node. | | | | | | | |
| ^{####} Source IP Address: The IP address of the sender or source node. | | | | | | | |
| ^{#####} Source Sequence Number: The current sequence number of the source node, which indicates the source sequence number in the routing table. | | | | | | | |

Table 2. Message format of Route Reply (RREP) request

| Type | R* | A** | Reserved*** | Prefix Size | Hop Count [@] |
|---|----|-----|-------------|-------------|------------------------|
| Destination IP Address [#] | | | | | |
| Destination Sequence Number ^{##} | | | | | |
| Originator IP address ^{###} | | | | | |
| Life Time ^{####} | | | | | |
| *R: Set the flag | | | | | |
| **Answer: Of course, | | | | | |
| ***Reserved: Sent as 0; ignore the answer. | | | | | |
| [@] Hop Count: The number of hops from the source IP address to the destination node IP address. | | | | | |
| Jumps: all jumps from target to target | | | | | |
| [#] Destination IP address: the IP address of the node that finally receives the data packet. | | | | | |
| ^{##} Destination Serial Number: The number of the receiving node. | | | | | |
| ^{###} Original IP Address: IP address of the meeting place. | | | | | |
| ^{####} Time: The specified time indicates when the packet should send its RREP to the request. | | | | | |

In a Mobile Ad hoc Network (MANET), if a source node has a malicious neighbor, it could receive a false reply to its request for a route to the destination. This false reply could falsely claim to have the shortest or minimum hop count route to the destination. Consequently, the source node may send its packet through this MN, which instead of forwarding it to the destination, simply drops it. This action prevents the source node from receiving an acknowledgment of packet delivery.

Since nodes in the network have limited energy resources, repeated attempts by the source node to send requests to neighboring nodes deplete its resources, while the MN keeps responding with false messages. This deception causes the source node to exhaust its resources and damages the entire network. The presence of a MN in a MANET can cause severe damage since it can deceive the source node into thinking it has found the shortest or minimum hop count route, ultimately depleted the network's energy resources and caused network failure.

For a proper introduction of MANET and the issues with its implementation and protocols, readers are encouraged to see (Shama et al., 2022; Rajendra et al., 2019; Suma et al., 2022; Shafi et al., 2023; Saetang et al., 2012).

Moundni et al. (2019) proposed using the (ANFIS) and (PSO) for detecting and preventing BHAs in (MANETs). The authors created a database using various input parameters and generated a neighbor table to monitor the neighborhood's activity to accomplish this. Their approach yielded positive results in detecting and preventing BHAs. However, the authors did experience some false alarms, indicating the detection of a BHA when none was present. Moundni et al.'s study demonstrated the effectiveness of ANFIS and PSO for detecting and preventing BHAs in MANETs. Despite some false alarms, their approach shows promise in improving the security of these networks.

Yaseen et al. (2018) incorporated a reputation table for each node in the network, allowing all nodes to access information about every other node. The reputation table is updated regularly to minimize the risk of BHAs, and the nodes move to different areas to avoid such attacks. The reputation table is created by allocating watchdog observations to each node in the network, using a low-overhead approach, which enables the watchdog to identify the shortest path to reach the destination. However, this watchdog technique has a drawback regarding low scalability, and its performance is subject to variation based on the network condition.

El-seminary et al. (2019) developed an enhanced version of the AODV routing protocol called the SAODV protocol, designed to provide improved security for mobile ad-hoc networks (MANETs) against BHAs. The authors utilized a chaotic map to enhance the security of the SAODV protocol. The SAODV protocol is more effective in preventing BHAs and can provide better protection against these attacks. Additionally, the SAODV protocol allows for grading against BHAs. Comparing the AODV and SAODV protocols revealed that the SAODV protocol is more secure and effective than the AODV protocol.

The author implemented PIHNSPRA routing algorithms to improve network efficiency and prevent data blockages. These algorithms help to find the most efficient path for transmitting data to end-to-end nodes. Additionally, Rajendran et al. (2019) utilized the priority component of the algorithm to manage nodes in mobile ad-hoc networks and prevent potential BHAs. The author also employed CniDsor techniques based on Intrusion Detection System (IDS) communication to further enhance route path efficiency. These techniques involve detecting the Attacker Detection Ratio (ADR) using various parameters to secure data transmission against BHAs, reducing overhead communication throughput, and increasing network lifetime.

Khmayseh et al. (2014) proposed several approaches for identifying BHAs in Mobile Ad-hoc Networks (MANETs), which can be used for proactive and reactive protocols. The authors suggested various techniques to detect and prevent such attacks, including the (CBDS), based on (DSR) protocols. CBDS identifies all nodes between the source and destination nodes by using RREP messages received from nodes in the network. Each node in the network sends an RREP message containing the sender node's address, indicating the network's activity. This approach aids in detecting BHAs and identifying MNs in the network.

Rani et al. (2020) introduced OBSA, an algorithm that comprises two components: ROBS (Route Observing transmissions) and REOS (Route Error Observer). The ROBS component involves both the source node and the observation node. The proposed solution was evaluated through simulations conducted in various scenarios. Specifically, the authors considered two scenarios in which 3 and 6 black holes were created. In the first scenario, a 3 black hole environment was simulated. The results indicated the simulation was efficient, particularly in dense networks with high mobility. In the second scenario, where 6 black holes were created, the observations were limited, and the only increase in

efficiency was observed in dense networks with higher mobility.

Syed et al. (2021) employed a machine-learning approach that utilized two types of classifiers: the (ANN) classifier and the (ABC) classifier. The ABC classifier was inspired by the intellectual activity of honeybees, allowing the authors to differentiate between nodes based on their behaviors and properties. The nodes were categorized into two lists, i.e., healthy and affected nodes. The authors utilized a node range of 50-100, with the network area covering 25% of the 1000*1000 mm². The models used were heterogeneous.

Shukla et al. (2021) analyzed various types of attacks that can occur in Mobile Ad-hoc Networks (MANETs) and also evaluated the performance metrics associated with such attacks. Furthermore, they discussed seven parameters essential for an ideal MANET. The paper comprehensively explains well-known MANET attacks such as Sybil, Flooding, and Black Hole. In addition, the authors also thoroughly discussed the concept of routing in MANETs, including the Optimization State Routing Protocol (OLSR) and Open System Path First (OSPF), as well as Multi-point Relays.

Nagalakshmi et al. (2021) presented a new system called ECCAODV based on an elliptic curve cryptosystem and AODV protocol. This system effectively removes two-dimensional attacks in mobile ad hoc networks, including wormhole and black hole attacks. The paper also discusses the limitations of the synchronization procedure and reset protocol movement through a data flow diagram. The study results show significant improvements over the MAODV protocol, including 75.97% energy savings and a 64.01% reduction in routing overhead.

Kumar et al. (2021) utilized machine learning models to detect BHAs in ad-hoc wireless networks. Specifically, they applied Random Forest and Decision Tree classifiers and performed a descriptive analysis of six Intrusion Detection Systems (IDSs), including ANOVA statistics. Parameters such as accuracy, detection rate, and false positive rate were used to evaluate the effectiveness of the IDSs. Moreover, the authors improved the IDSs to counter additional types of attacks that may occur in the network.

Gaurav et al. (2021) presented a secure AODV routing algorithm for detecting BHAs in vehicular ad-hoc networks. The researchers made slight improvements to the RREQ and RREP packet protocols and used NS-2.33 simulators to validate their scenario and results. The study successfully demonstrated the ability to detect and remove infected nodes from the network, and the

network's throughput was evaluated using performance metrics. Specifically, the researchers used the Packet Delivery Ratio (PDR) to analyze the flow of data packets in the network.

Shah et al. (2021) proposed a lightweight prevention approach for securing Mobile Ad-hoc Networks (MANETs) by constructing a secure backbone. The approach allowed for the detection of attacks without excessively draining the resources of individual nodes. The researchers employed various security mechanisms to identify black and grey-hole attacks and demonstrated the effectiveness of their BTRES approach in detecting BHAs. The study utilized an NS-2 simulator to obtain results. However, the authors acknowledged that there is still room for improvement in the algorithm.

Oakley et al. (2020) introduced a Detection and Prevention System (DPS) node designed to detect BHAs in Mobile Ad-hoc Networks (MANETs). The study focused on analyzing the packet drop frequency of single and dual black hole nodes, which can lead to network degradation and affect the network's performance.

Li et al. (2019) surveyed solutions to BHAs in MANETs. They discussed using OLSR, RPL, and reactive protocols such as DSR and AODV to prevent BHAs. The paper summarized the proposed schema for addressing BHAs and compared various solutions. However, the authors noted that more analysis is needed. The Packet Delivery Ratio (PDR) was used to show how many packets are successfully delivered in the network.

Khalaf et al. (2020) proposed a method called DAPV for detecting malicious activity in mobile ad-hoc networks (MANETs). They utilized NDlog to identify any abnormal behavior in the network and used DAPV to illustrate the direction of the malicious activity by plotting a graph. However, implementing this approach in real-life scenarios may pose challenges and consume considerable time.

Similarly, Cai et al. (2018) suggested an improved MANET structure that employs a bait system to detect and prevent black and grey-hole attacks. To simulate the MANET scenarios, they used the NS-2 simulator and developed a performance matrix to evaluate the efficiency of their proposed system, called CBDS. The results showed that CBDS could sustain the entire network for half of the MNs, which typically causes network depletion.

In their recent study, Pranav et al. (2021) highlighted that while mobile ad-hoc networks (MANETs) are widely used due to their ease of deployment, they also present a security risk as they can be vulnerable to attacks that compromise network security and steal sensitive

information. The authors proposed three evolutionary self-cooperative trust detection systems to address this challenge to prevent real-time cooperative BHAs. The proposed systems work by continuously monitoring the MANET for any suspicious activities. If any malicious activity is detected, the system immediately alerts the source node and relevant nodes in the network to prevent the attack. The system also generates a Packet Delivery Ratio (PDR) report to provide accurate information on the malicious activity. The authors reported that the system could detect and prevent up to 90% of the DSR routing attacks with high accuracy.

Black Hole Attack

A BHA is a security threat in mobile ad hoc networks (MANETs) where a MN attracts and drops all the data packets in the network by advertising itself as having the shortest path to the destination. In a MANET, nodes communicate with each other directly, without the need for a centralized infrastructure. This decentralized architecture makes it vulnerable to attacks, including the BHA.

In a BHA, the MN creates a false route advertisement (RREQ) packet, indicating that it has the shortest path to the destination. Other nodes in the network trust the information provided by this node and send their data packets to it. However, instead of forwarding the packets to the destination, the MN simply drops them. This results in a loss of data packets, and the legitimate nodes in the network are unable to communicate with each other. One of the main challenges in detecting a BHA is that the MN can easily modify the routing protocol messages to make them appear legitimate. Therefore, several techniques have been proposed to detect and prevent BHAs in MANETs. These techniques include monitoring the behavior of nodes, using trusted nodes to monitor the network, and using cryptographic techniques to secure the communication between nodes. BHA is a severe security threat in MANETs that can disrupt the communication between nodes and cause data loss. It is essential to deploy appropriate security mechanisms to prevent and detect such attacks and ensure the secure and reliable operation of MANETs.

The diagram in Figure 1 depicts a dynamic topology within a network that comprises ten interconnected nodes. The network has a source node and a destination node, and when the source node intends to send data packets to the destination node, it broadcasts a RREQ message to discover the shortest path. However, in the presence of a MN or a black hole node, such as node 4, the RREQ message is intercepted, and a fake RREP

message is instantly sent to the source node, which is node 1 in this case. After receiving the RREP message, node 1 follows the suggested routing path and sends the data packets. Unfortunately, the MN (node 4) receives and discards the data packets, resulting in a significant degradation of the network's performance. There are two types of BHAs: the simple BHA and the cooperative BHA.

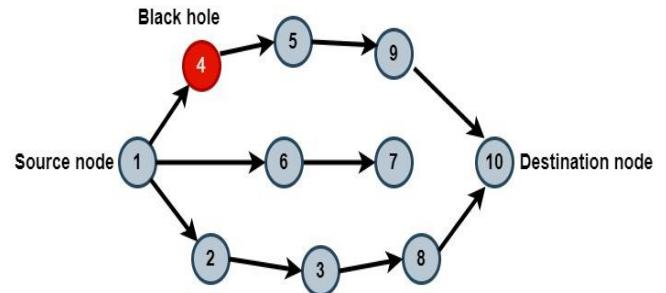


Figure 1. Black Hole Attack

Simple BHA

In a simple BHA, a single node within a network engages in malicious activity. This node intercepts and discards all data packets passing through the network, leading to depletion of the network's resources. Whenever a RREQ is broadcasted to retrieve data packets, the MN responds instantly with a false RREP, without verifying the actual path to reach the destination.

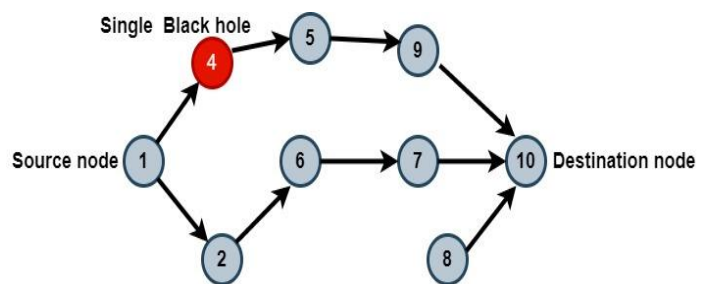


Figure 2. Single BHA

Figure 2 portrays an attack in which a harmful node, node 4, employs a routing method to propagate messages throughout the network. The MN waits and keeps track of when the source node, node 1, solicits a RREQ for the quickest way to reach the destination. Each time the source node sends a RREQ, node 4 expeditiously dispatches a counterfeit RREP to the source node without authenticating the routing table. This deceptive response is treated as the most direct path for message transmission, causing the data packets to be diverted towards the MN, which interferes with the network's performance.

Cooperative BHA

In a MANET, nodes communicate with each other through wireless connections without the need for a pre-existing infrastructure. However, this also makes

MANETs vulnerable to attacks, including the BHA. A BHA is a type of Denial of Service (DoS) attack, in which a MN falsely advertises itself as having the shortest path to the destination node, thereby intercepting and dropping all incoming packets, making the destination node unreachable. In a Cooperative black hole attack, multiple malicious nodes work together to launch the attack. In this scenario, each MN claims to have the shortest path to the destination, and they collaborate to drop the packets. This makes it difficult for the other nodes in the network to detect the attack and avoid the MNs. To prevent Cooperative BHAs in MANETs, various countermeasures have been proposed, such as the use of secure routing protocols, detection algorithms, and cryptographic techniques. These techniques aim to identify and isolate the MNs in the network, thereby preventing them from disrupting the communication among the legitimate nodes.

The situation at hand involves a network that has been infiltrated by multiple nefarious nodes that are collaborating to carry out harmful activities. Whenever a transmitting node tries to send data packets, it sends a broadcast message called a RREQ to the network. However, the MNs, M1 and M2, intercept the RREQ message and reply with a counterfeit RREP message to the designated receiver node. Working together in the network, M1 and M2 pursue their malevolent goals, which cause harm to the network as a whole.

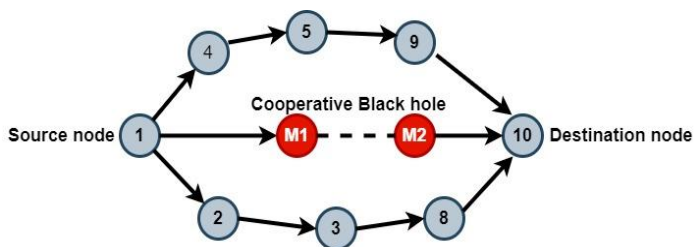


Figure 3. Cooperative BHA

In Figure 3, a cooperative BHA is depicted where two MNs, namely M1 and M2, are present in the network. The attack begins when node 1, the source node, sends (RREQ) in the network to locate the destination node. In this scenario, M1 and M2 respond to node 1 without actually computing the correct path to the destination node. The MNs work in tandem and collaborate with each other to execute their nefarious actions in the network. Once M1 and M2 receive the data packets, they discard them, causing severe disruption in the network's performance. These MNs maintain constant communication with each other and produce fake routing replies (RREP) to the source node, misleading it about the location of the destination node. This attack significantly deteriorates the network's functionality.

Methodology

This paper presents a new approach for detecting and preventing BHAs, utilizing two sub-methods.

- The first sub-method involves implementing Andrews's plot to identify any potentially harmful behavior within the network.
- The second sub-method entails assigning credibility to nodes, thereby preventing senders from transmitting their packets to any MNs.

Detection of BHA Activity in MANET Using Andrews Plot

Andrews plot, also known as Andrew's curve, is a visualization technique introduced by Andrews et al. (1972) for projecting multidimensional data onto a two-dimensional plot. The plot can accommodate both integer and non-integer values and is sometimes referred to as a Fourier curve because it uses a Fourier basis to display multi-dimensional points into a single profile.

The Andrews curve represents each data point as a curve in a two-dimensional plane. The curve is generated by applying a Fourier series to the original data, where each coefficient of the Fourier series is determined by the original data's values. The resulting curve represents a projection of the original data onto a two-dimensional plane. The Andrews plot is particularly useful for comparing different datasets because it allows one to visualize the shape of the curves and compare them directly. The method is often used in data analysis, machine learning, and signal processing. Andrew's plot is a visualization technique used to project multidimensional data onto a two-dimensional plot. The plot represents each data point as a curve generated using a Fourier series. The method is commonly used in data analysis, machine learning, and signal processing to compare different datasets.

$$f(x) = \frac{x_1}{\sqrt{2}} + x_2 \sin(t) + x_3 \cos(t) + x_4 \sin(2t) + x_5 \cos(2t) + \dots \quad (1)$$

Equation (1) is plotted over the interval of $-\pi < t < \pi$ in our scenario, where we utilize Andrew's plot based on node credibility, as introduced by Andrews et al. (1972).

To apply Andrew's plot in our scenario, we use the variable x_i to represent the node credibility of each transaction. We can use equation (1) to project these data points into a vector, where x represents the node credibility, and t varies from -3.14 to $+3.14$.

In our scenario, we apply Andrew's plot based on node credibility, where each transaction's credibility is represented by the variable x_i . Equation (1) is used to project the data points into a vector, where x represents the node credibility, and t varies from -3.14 to $+3.14$.

Prevention of BHA Using Node Credibility

Table 3. 3 Transactions of Node Credibility Calculation

| Node | Hop counts | Credibility | Waiting for the 0.005-time stamp after transmitting once. | 2 transmission and waiting for the 0.005-time stamp | 3 transmission and waiting for the 0.005-time stamp |
|------|------------|-------------|---|---|---|
| 1 | $1*5=5$ | 5 | 5 | 5 | 5 |
| 2 | $1*5=5$ | 5 | 5 | 5 | 5 |
| 3 | $1*5=5$ | 5 | 5 | 5 | 5 |
| 4 | $1*5=5$ | 5 | $5-1=4$ | $4-1=3$ | $3-1=2$ |
| 5 | $1*5=5$ | 5 | 5 | 5 | 5 |

The Calculation for the Nodes Credibility

When a Mobile Ad hoc Network (MANET) is formed, there are source and destination nodes. When the source node needs to transmit data packets, it sends a broadcast message called the RREQ to find a route to the destination node. Unfortunately, a MN may also be waiting for such messages in the network. Upon receiving the RREQ message, the MN responds with a fake RREP without calculating the proper path to the destination node. Unaware of the deceitful message, the source node believes it and sends the data packets to the MN. The MN collects and drops the packets, leading to network depletion.

We have proposed a method to enhance the security of Mobile Ad-hoc Networks (MANETs) by introducing the concept of node credibility. This approach involves categorizing the nodes in the network as either good, suspicious, or malicious based on their credibility levels, which are determined using fuzzy rules. Nodes with high credibility are classified as good, while those with medium credibility are considered suspicious. Nodes with low credibility levels are marked as malicious and treated accordingly. This approach aims to improve the overall security of the MANETs by identifying potentially harmful nodes and taking appropriate action to mitigate their impact on the network

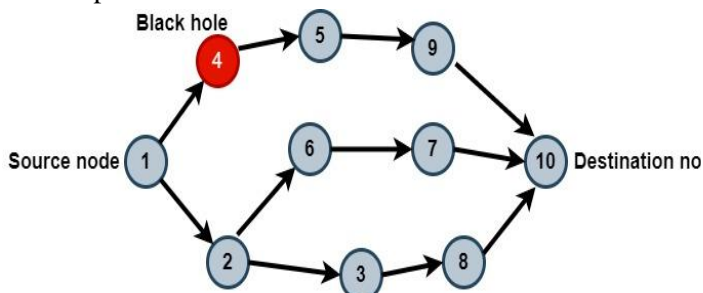


Figure 4. For Calculating Credibility of Nodes in MANET

Steps for calculating the node credibility in MANET

1. At the beginning, all nodes in a MANET are interconnected.
2. In order to prevent BHAs within the AODV routing protocol, a credit system has been implemented to determine the reliability of each node.
3. The routing request (RREQ) message is broadcasted by the source node throughout the network.
4. Assuming a one hop distance between the source node (node 1 in figure 4) and its adjacent nodes, nodes 2 and 4.
5. Likewise, nodes 2 and 4 have a one hop distance to their respective adjacent nodes within the network.
6. In Figure 4, when node 1 broadcasts a request message for the RREQ, every node in the network is given 3 credits each, as specified in Table 3.
7. A MN in the network may provide a fake RREP to node 1.
8. Upon receiving the fake RREP, node 1 checks the shortest route to the destination node.
9. By examining the routing table, node 1 selects the MN as the next hop to send the packets.
10. The MN, upon receiving the packets, drops them from the network.
11. Conversely, genuine nodes compute the distance to the destination node and provide a genuine RREP.
12. By following the authentic path indicated in the routing table, nodes receive credits based on their route selection and forward the packets accordingly.
13. Node 2 sends the data packets to its neighboring nodes, assuming a hop count of 1. The neighbors of node 2, in turn, assign the hop count to their respective neighbors as the packets move further.
14. If the source node, node 1 from fig 4, does not receive the credit acknowledgment (CACK) message for the 0.005-time stamp from the destination node, it will reduce its node credit by one as shown in table 1. This

decrease in the node's credibility is attributed to the last node through which the message was sent.

15. Once the message arrives at the destination node, it will send the credit acknowledgment (CACK) to its neighboring node, bypassing the adjacent node. This CACK message will continue to propagate through the network until it reaches the source node. As a result, the source node's credibility will increase by a factor of 2, which helps to improve the overall credibility of the nodes.

16. Nodes with higher credibility are considered more trustworthy and reliable for data transmission and communications. Therefore, the credibility of a node is a crucial factor in determining its ability to participate in the network and play a vital role in ensuring smooth and efficient communication.

To simulate our proposed system, we established the following three rules:

Fuzzy rules

Rule 1: If a node's credibility is classified as high, then it is categorized as a good node.

Rule 2: If a node's credibility is classified as medium, then it is considered a suspicious node.

Rule 3: If a node's credibility is classified as low, then it is identified as a MN.

Fuzzy rules are rule-based systems that use fuzzy logic to handle imprecise, uncertain, or ambiguous data. Fuzzy rules are beneficial when traditional rule-based systems, such as decision-making, control systems, robotics, and artificial intelligence, are inadequate. Here are some of the reasons why fuzzy rules are commonly used:

Handling imprecise data: Fuzzy rules are particularly useful when the data is imprecise or uncertain. Fuzzy logic can handle data that is not precisely quantifiable and assign degrees of truth to linguistic variables. This makes fuzzy rules suitable for modeling systems with vague or ambiguous inputs, such as language or human behavior.

Handling complex systems: Fuzzy rules are a flexible and intuitive way to model complex systems that involve multiple inputs and outputs. A fuzzy system can perform sophisticated reasoning and decision-making tasks by combining various fuzzy rules. Fuzzy rules can handle complex interactions between variables, which is challenging using traditional rule-based systems.

Handling noise and errors: Fuzzy logic allows for a degree of uncertainty in the data, which makes it more robust to noise and errors. Fuzzy rules can still produce meaningful results even when the input data has some imprecision. This makes fuzzy rules a good choice for

systems that operate in noisy environments, such as robotics or control systems.

Expert knowledge representation: Fuzzy rules can represent specialist knowledge more naturally than traditional rule-based systems. Linguistic variables and rules written in a natural language make it easier for domain experts to specify their understanding. Fuzzy rules can capture the intuition of experts more naturally and produce more meaningful results.

Ease of implementation: Fuzzy rules are easy to implement and do not require a lot of computational resources. This makes fuzzy rules a good choice for real-time systems with critical response time.

Fuzzy rules are a powerful tool for modeling and reasoning in situations where the available information is imprecise, uncertain, or ambiguous. They are instrumental in complex systems, noisy environments, and situations where expert knowledge needs to be represented naturally. Fuzzy rules are easy to implement and can produce meaningful results even when the data is not quantifiable.

Fuzzy logic is a computing paradigm that deals with reasoning and decision-making in situations that involve uncertainty, ambiguity, and imprecision. Fuzzy logic allows for an approximate reason, where the truth value of a statement is represented by a degree of membership in a fuzzy set rather than a binary value (true or false).

The architecture of a fuzzy logic system can be divided into four main components:

Fuzzifier: Fuzzifier converts input data (such as sensor measurements) into fuzzy sets. A fuzzy set is defined by a membership function that assigns a degree of membership to each element in the set. The membership function can be defined in various ways, such as triangular, trapezoidal, or Gaussian shapes. The degree of membership reflects the degree to which the input value belongs to the fuzzy set.

Rule Base: The rule base contains a set of rules that define how to make decisions based on the fuzzy sets generated by the Fuzzifier. Each rule consists of an antecedent (input condition) and a consequent (output action). The antecedent is expressed in fuzzy sets, and the consequent defines the degree to which a particular action should be taken based on the input conditions. Fuzzy rules are a rule-based system used in fuzzy logic, a mathematical framework for dealing with uncertainty and imprecision in data. Fuzzy rules are used to model complex systems where the inputs and outputs are not precisely defined or where there is a degree of ambiguity in the relationships between inputs and outputs. A fuzzy rule consists of two parts: an antecedent and a consequent. The antecedent specifies the conditions under which the rule applies and the consequent

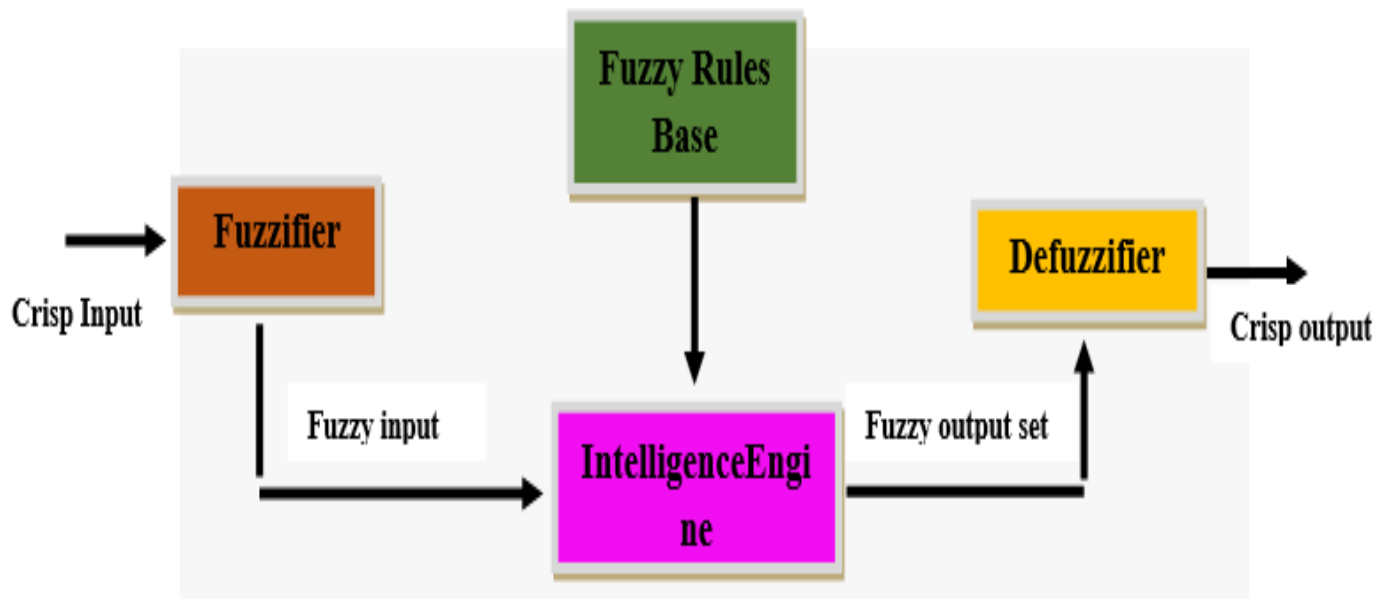


Figure 6. The Architecture of Fuzzy Logic

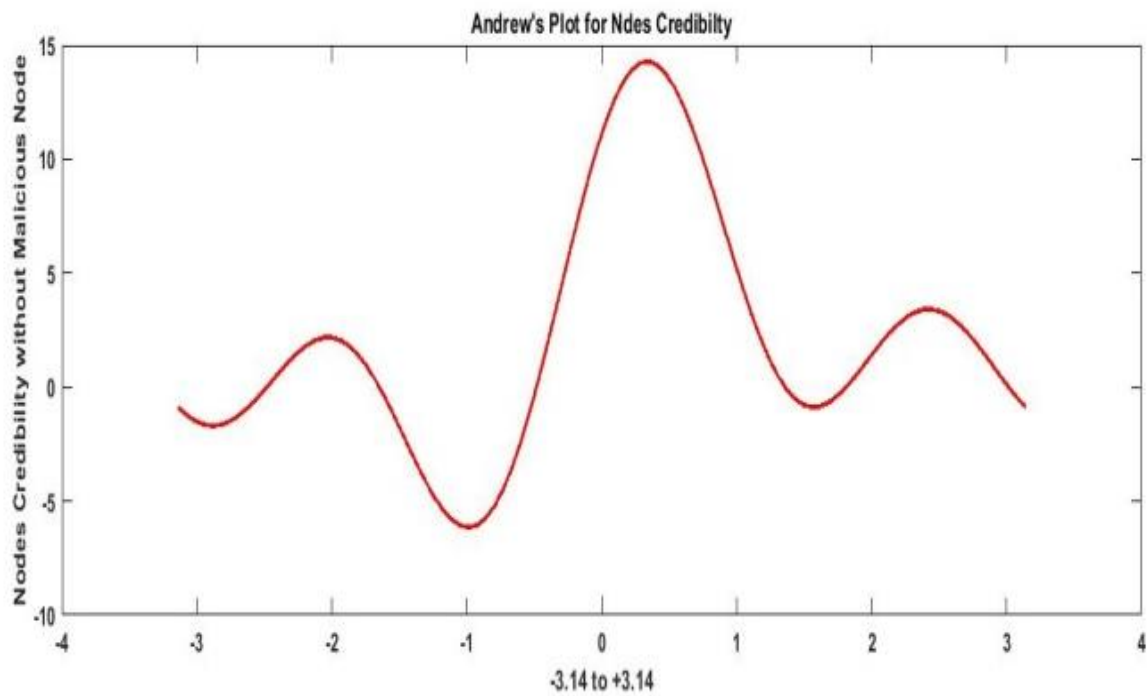


Figure 5. Andrews Plot without black hole nodes

specifies the action to be taken if the antecedent is true. Fuzzy rules are often written in the form "IF <antecedent> THEN <consequent>," where the antecedent and consequent are expressed using fuzzy sets. Fuzzy sets generalize classical (or crisp) settings, containing only elements that satisfy a precise definition. In contrast, fuzzy sets allow elements to have a degree of membership in the set, represented by a value between 0 and 1. This degree of membership reflects the degree to which an element possesses the characteristics of the set. In a fuzzy rule, the antecedent is typically expressed as a combination of fuzzy sets using logical operators such as AND, OR, and NOT. The fuzzy sets represent the values of the inputs to the system, and the logical operators combine these values to form a single value that represents the degree to which the antecedent is true. The consequent of a fuzzy rule is expressed using a fuzzy set that represents the system's output. The fuzzy set is

contrast, the Sugeno method uses a weighted average of the consequences.

d. Defuzzifier: The defuzzifier converts the fuzzy output sets generated by the inference engine into crisp output values. This is done by computing a weighted average of the output fuzzy sets, where the weights are determined by the degree of membership in each fuzzy set. The crisp output value represents the final decision or action that the system should take.

The architecture of a fuzzy logic system is flexible and can be adapted to a wide range of applications, including control systems, decision-making systems, and pattern recognition systems. Fuzzy logic has the advantage of being able to handle imprecise and uncertain data, which makes it particularly useful in situations where traditional logic and rule-based systems are inadequate.

$$fx(t) = \frac{3}{\sqrt{2}} + 3 \sin(t) + 3 \cos(t) + 3 \sin(2t) +$$

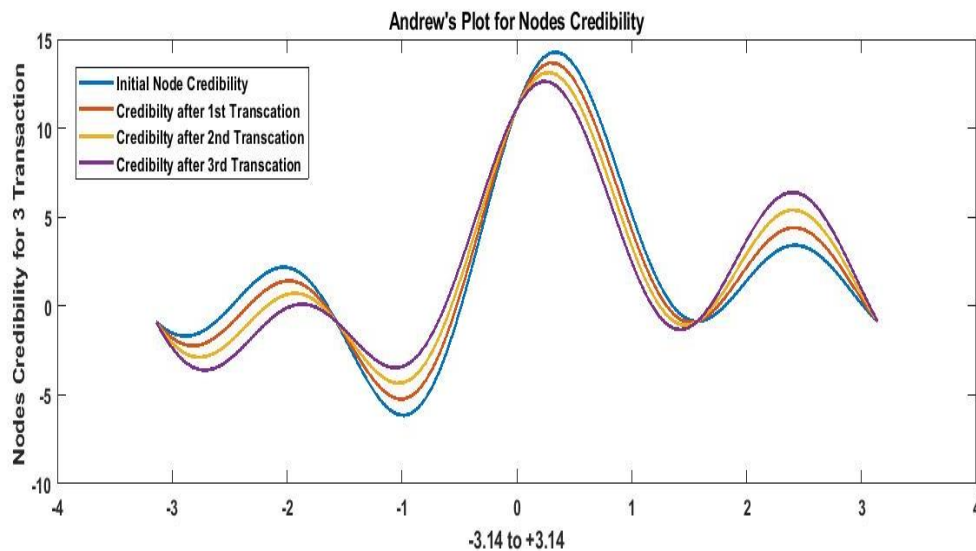


Figure 7. Andrews plot for detection of BHA

defined by a membership function that maps input values to output values. The membership function is typically determined using expert knowledge or data from the modeled system. Fuzzy rules are used in various applications, including control, decision-making, and pattern recognition systems. They provide a flexible and intuitive way to model complex systems and handle uncertainty and imprecision in data.

c. Inference Engine: The inference engine applies the rules in the rule base to the fuzzy sets generated by the Fuzzifier to derive a set of fuzzy output sets. Different methods of combining the rules exist, such as the Mamdani or the Sugeno method. The Mamdani method uses fuzzy set operations such as intersection and union to connect the antecedent and consequent of each rule. In

$$3 \cos(2t) + \dots (2)$$

In order to test the accuracy of the formulated fuzzy rules, a simulation was conducted using MATLAB version R2021b and a scenario was created in Network Simulator, focusing on a MANET setting. Andrews's plot was employed, which involves projecting multi-dimensional points into two-dimensional ones. The 'here' variable was used, with a range of -3.14 to +3.14, as per Equation (2) in the plot. It was observed that in the absence of any malicious activity in the MANET, the Andrews curve remained unchanged even after multiple transactions were conducted within the network. This curve serves as an indicator of the trustworthiness and reliability of the nodes in the network, with high credibility indicating that the nodes are dependable and trustworthy. The fuzzy rules were then utilized to identify

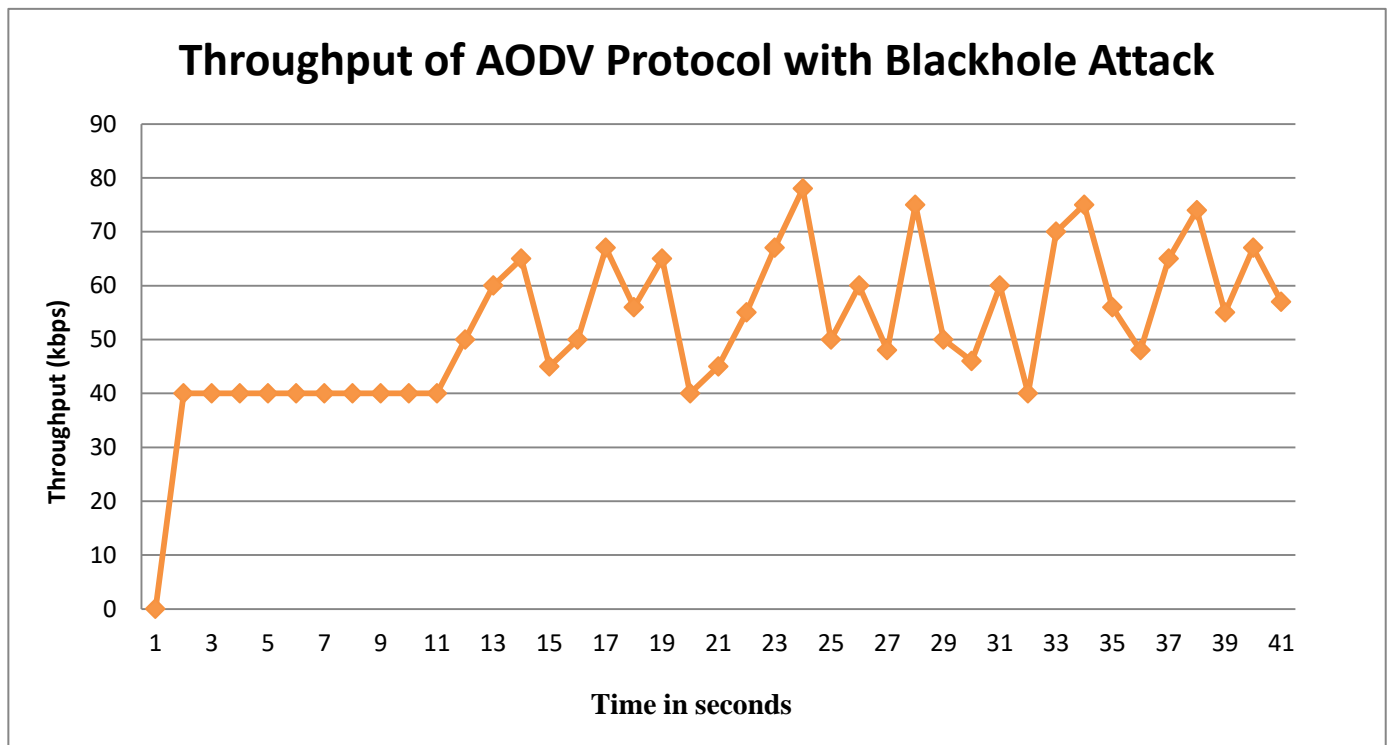


Figure 8. Throughput of MANET with BHA

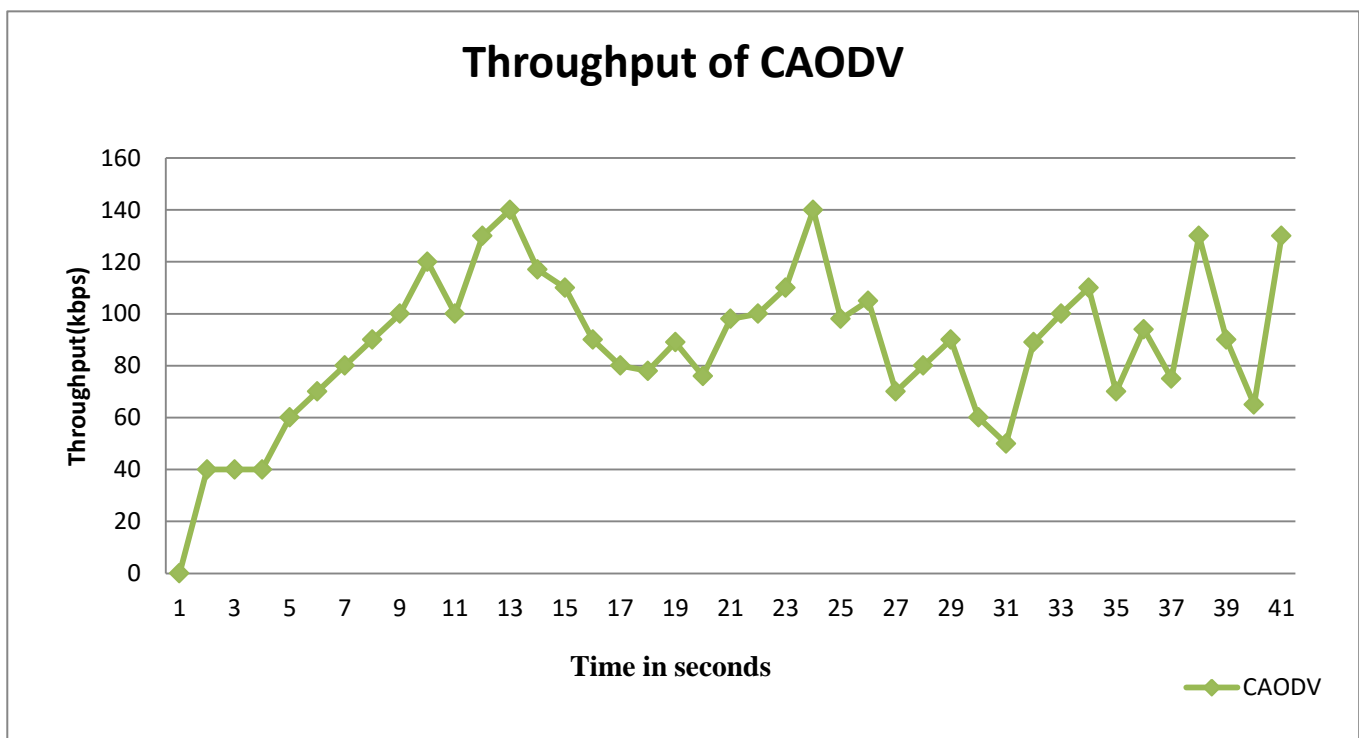


Figure 9. Throughput of MANET using node credibility in AODV protocol

the nodes with high credibility, which were considered to be more trustworthy and reliable within the network.

$$fx(t) = \frac{x_1}{\sqrt{2}} + x_2 \sin(t) + x_3 \cos(t) + x_4 \sin(2t) + x_5 \cos(2t) + \dots (3)$$

Equation 3 is an Andrews plot equation that helps to project multi-dimensional points into two-dimensional projections. In this equation, 'x' denotes node credit, while 't' ranges from -3.14 to +3.14. In a MANET (MANET), the source node initiates the RREQ message

inferred that the credibility of node 4 from figure 4 and table 1 has decreased. This suggests that node 4 has moderate credibility and is potentially suspicious. As the network's data packets undergo a second transaction, the credibility of node 4 continues to decrease, indicating that it is a MN and that a BHA has occurred in the network. The source node has been informed about the presence of MNs.

The above fig 8 shows that the network's throughput decreased while the BHA was there. If the network throughput is declining, that shows that some malicious

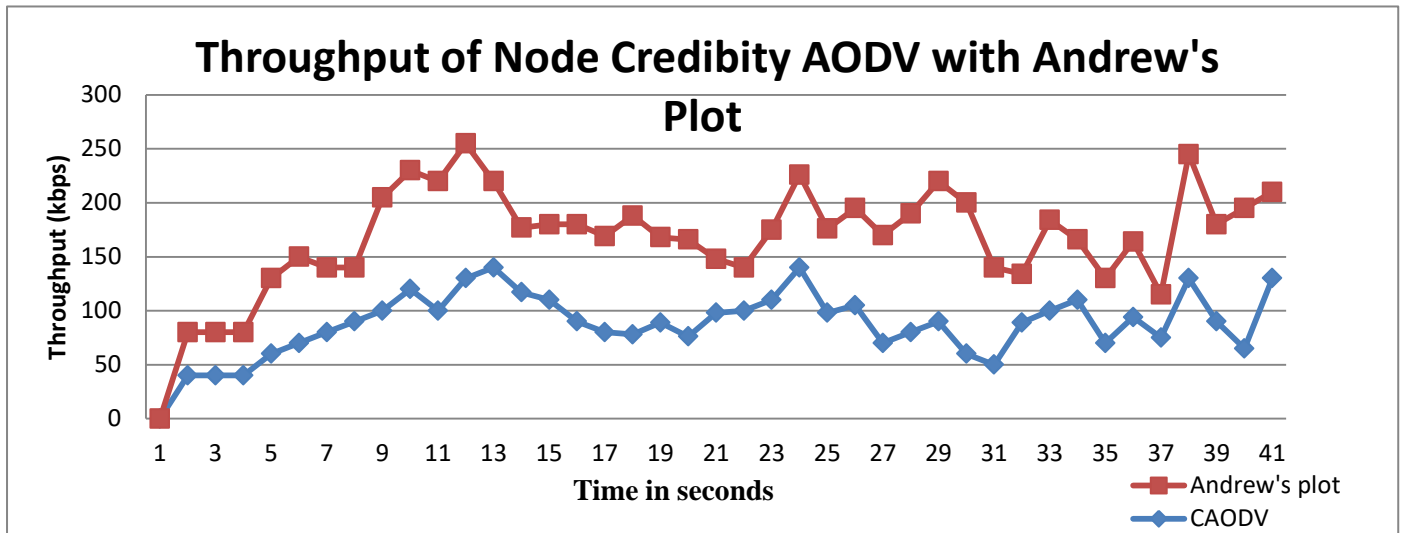


Figure 10. Throughput of MANET using node credibility with Andrew's plot.

to locate the destination node. High node credit indicates the absence of malicious activity in the network. However, when a MN enters the network, it starts broadcasting fake RREP messages to the source node, misleading it that the fake path is the shortest route to the destination. The source node trusts this reply and sends data packets through this fake path. Upon receiving the data packets, the MN drops them from the network, causing depletion of the network resources. The source node awaits delivery confirmation from the destination node, which it never receives due to the MN's actions.

To prevent such malicious activities, the Andrews plot is used. Andrew's plot detects malicious activities in the network by observing changes in the plot's curves over time. After a few data transactions, the MN's actions will alter the plot's curves, indicating suspicious activity in the network. By detecting such changes, appropriate measures can be taken to prevent the network from depleting.

After the first transaction in the MANET

$$fx(t) = \frac{3}{\sqrt{2}} + 3 \sin(t) + 3 \cos(t) + 2 \sin(2t) + 3 \cos(2t) + \dots (4)$$

Based on equation 4, where x represents node credibility, and t varies from -3.14 to +3.14, it can be

activity is going on, which decreases the network performance. That indicates that the data transmission on that path is not safe.

Fig 9 shows that when there is a BHA in the network. The throughput of the network decreases. For detecting the BHA in the network, node credibility is proposed, which helps the network administrator to manage the network and its performance. When node credibility is implemented in the network to detect BHAs, the thought of the network starts increasing; this shows that the network is becoming more secure for data transmission and communication. From the previous work by Saetang et al. (2012), we also used credibility to detect BHAs in MANET. In that paper, their network throughput is increased by 40%, but in our network, throughput is increased up to 90%, which shows that our technique is more helpful in securing the network from BHAs. With the help of Andrew's plot, we plot the graph through which we can visualize which network area is attacked by the BHA shown in Figure 8.

The above figure 10 shows that MANET throughput is increased, which indicates that the network is more secure and safe for data transmission and communication—Andrew's plot help in visualizing which

part of the network is attacked by the BHA. Andrews's plot can be particularly useful in identifying clusters and patterns in multivariate data sets and detecting outliers. It can also be used as a dimensionality reduction technique, where the plot can be used to visualize the data in two dimensions, making it easier to understand and interpret. Andrews's plot is a simple and effective way to visualize multivariate data and can be helpful for exploratory data analysis.

Conclusion and future work

This paper presents two techniques for addressing BHAs in (MANETs): one for detection and another for prevention. In the detection method, the credibility of nodes is utilized to detect any potential attacks. The prevention method employs Andrews's plot to assess the node's credibility. The node's credibility is evaluated after three transactions in the network, and the nodes are marked as good, suspicious, or malicious based on fuzzy rules. The node's credibility is determined by plotting the graph of three transactions, and any malicious activity in the network is identified. If all Andrews plot curves coincide, even after multiple transactions, it indicates no malicious activity in the network. Conversely, if Andrew's plot curves do not coincide, it implies malicious activity in the network.

Acknowledgements

I would like to thank Birla Institute of Technology, Mesra for providing me the basic infrastructure to carry out the research. I would like to give my sincere thanks to the reviewers whose positive comments improved my manuscript. Finally, I would like to thank the Editorial Team of International Journal of Experimental Research and Review for giving me a platform to publish my work.

Conflict of interest

The authors declare that they do not have any conflict of interest

References

Andrews, D.F. (1972). Plots of high-dimensional data. *Biometrics*, 28, 125-136.
<https://doi.org/10.2307/2528964>

Cai, R. J., Li, X. J., & Chong, P. H. J. (2018). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. *IEEE transactions on Mobile Computing*, 18(1), 42-55.
<https://doi.org/10.1109/TMC.2018.2828814>

Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2014). Defending against collaborative attacks by malicious nodes in MANETs: A

cooperative bait detection approach. *IEEE Systems Journal*, 9(1), 65-75.
<https://doi.org/10.1109/JSYST.2013.2296197>

El-Semary, A. M., & Diab, H. (2019). BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access*, 7, 95197-95211.
<https://doi.org/10.1109/ACCESS.2019.2928804>

Gaurav, A., & Singh, A. K. (2021). Light weight approach for secure backbone construction for MANETs. *Journal of King Saud University-Computer and Information Sciences*, 33(7), 908-919. <https://doi.org/10.1016/j.jksuci.2018.05.013>

Khalaf, O. I., Ajesh, F., Hamad, A. A., Nguyen, G. N., & Le, D. N. (2020). Efficient dual-cooperative bait detection scheme for collaborative attackers on mobile ad-hoc networks. *IEEE Access*, 8, 227962-227969.
<https://doi.org/10.1109/ACCESS.2020.3045004>

Khamayseh, Y. M., Aljawarneh, S. A., & Asaad, A. E. (2018). Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. *Sustainable Computing: Informatics and Systems*, 18, 90-100.
<https://doi.org/10.1016/j.suscom.2017.07.001>

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, 80, 103352.
<https://doi.org/10.1016/j.micpro.2020.103352>

Li, T., Ma, J., Pei, Q., Song, H., Shen, Y., & Sun, C. (2019). DAPV: Diagnosing anomalies in MANETs routing with provenance and verification. *IEEE Access*, 7, 35302-35316.
<https://doi.org/10.1109/ACCESS.2019.2903150>

Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2019). Black hole attack detection using fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, 151, 1176-1181.
<https://doi.org/10.1016/j.procs.2019.04.168>

Nagalakshmi, T. J., Gnanasekar, A. K., Ramkumar, G., & Sabarivani, A. (2021). Machine learning models to detect the blackhole attack in wireless adhoc network. *Materials Today: Proceedings*, 47, 235-239.
<https://doi.org/10.1016/j.matpr.2021.04.129>

Oakley, I. (2020). Solutions to Black Hole Attacks in MANETs. *IEEE*, In *2020 12th International*

Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 1-6.

<https://doi.org/10.1109/CSNDSP49049.2020.9249524>

Pranav, P., Dutta, S., &Chakraborty, S. (2021).Empirical and statistical comparison of intermediate steps of AES-128 and RSA in terms of time consumption. *Soft Computing*, 25(21), 13127-13145. <https://doi.org/10.1007/s00500-021-06085-6>

Rajendran, N., Jawahar, P. K., &Priyadarshini, R. (2019). Cross centric intrusion detection system for secure routing over black hole attacks in MANETs. *Computer Communications*, 148, 129-135. <https://doi.org/10.1016/j.comcom.2019.09.005>

Rani, P., Verma, S., & Nguyen, G. N. (2020). Mitigation of black hole and grayhole attack using swarm inspired algorithm with artificial neural network. *IEEE Access*, 8, 121755-121764. <https://doi.org/10.1109/ACCESS.2020.3004692>

Saetang, W., &Charoenpanyasak, S. (2012).Caodv free blackhole attack in ad hoc networks. IACSIT Press., In *International Conference on Computer Networks and Communication Systems (CNCS 2012) IPCSIT*, 35, 63-67.

Shafi, S., Mounika, S., &Velliangiri, S. (2023). Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET. *Procedia Computer Science*, 218, 2309-2318. <https://doi.org/10.1016/j.procs.2023.01.206>

Shah, I. A., &Kapoor, N. (2021).To Detect and Prevent Black Hole Attack in Mobile Ad Hoc Network.

IEEE, In *2021 2nd Global Conference for Advancement in Technology (GCAT)*, pp. 1-4. <https://doi.org/10.1109/GCAT52182.2021.9587471>

Sharma, D. K., Dhurandher, S. K., Kumaram, S., Gupta, K. D., & Sharma, P. K. (2022). Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. *Computer Communications*, 189, 182-192. <https://doi.org/10.1016/j.comcom.2022.04.003>

Shukla, M., & Joshi, B. K. (2021).WITHDRAWN: A novel approach using elliptic curve cryptography to mitigate Two-Dimensional attacks in mobile Ad hoc networks. *Materials Today: Proceedings*, <https://doi.org/10.1016/j.matpr.2020.12.886>

Suma, S., &Harsoor, B. (2022).An approach to detect black hole attack for congestion control utilizing mobile nodes in wireless sensor network. *Materials Today: Proceedings*, 56, 2256-2260. <https://doi.org/10.1016/j.matpr.2021.11.590>

Syed, S. A. (2021). WITHDRAWN: A systematic comparison of mobile Ad-hoc network security attacks. Syed, S.A. (2021). A systematic comparison of mobile Ad-hoc network security attacks. *Materials Today: Proceedings*, <https://doi.org/10.1016/j.matpr.2020.12.617>

Yaseen, Q. M., &Aldwairi, M. (2018).An enhanced AODV protocol for avoiding black holes in MANET. *Procedia Computer Science*, 134, 371-376. <https://doi.org/10.1016/j.procs.2018.07.196>

How to cite this Article:

Ankita Kumari, Sandip Dutta and Soubhik Chakraborty (2023). Use of Node credibility and Andrews plot to detect and prevent BHA in MANET. *International Journal of Experimental Research and Review*, 30, 282-295.

DOI : <https://doi.org/10.52756/ijerr.2023.v30.026>



This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.