International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223693 Volume 10, Issue 6, November – December (2023)

RESEARCH ARTICLE

ANFIS-RSOA Approach for Detecting and Preventing Network Layer Attacks in MANET

Sivanesan N
Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advance Studies (VISTAS), Chennai, Tamil Nadu, India.
profnsivanesan@gmail.com

Rajesh A
Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advance Studies (VISTAS), Chennai, Tamil Nadu, India.
arajesh.se@velsuniv.ac.in

K. S. Archana
Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India.
archanak1@srmist.edu.in

Received: 26 August 2023 / Revised: 18 October 2023 / Accepted: 09 November 2023 / Published: 30 December 2023

Abstract – The primary obstacle typically encountered in Mobile Ad hoc Networks (MANETs) pertains for mitigating the impact of attacks prompted through malevolent nodes or identify promptly as well as addressing the certain nodes presence. This paper presents a hybrid technique in assault detection present in the context of MANETs. The research work focuses on addressing the challenge present in the MANET by introducing the robust Intrusion Detection System (IDS) using hybrid Machine Learning (ML) methods. The proposed approach for identifying attacks involves the utilization of the Adaptive Neuro Fuzzy Inference System in conjunction with the Rat Swarm Optimization Algorithm (ANFIS-RSOA). Hence, this hybrid ML approach has capability to produce high secure with precise and reliable outcomes. The suggested protocols concentrate on the security within a network by effectively identifying and mitigating potential assaults. The suggested methodology is executed within the NS2 platform and afterwards compared to various conventional methodologies, namely (PSO) Particle Swarm Optimization, (WOA), Whale Optimization Algorithm and Grey Wolf Optimization Algorithm (GWO). In order to evaluate the efficacy of the suggested methodology, it is subjected to testing using two distinct types of attacks, namely the (BHA) Black Hole Attack and the Wormhole Attack (WHA). This proposed ANFIS-RSOA method performance metrics such as jitter, throughput, delay, Packet Delivery Ratio (PDR), and low end-to-end delay is evaluated and compared with existing IDS methods. Moreover, the purpose of study is to protect both individual network nodes and their connections to one another.

Index Terms – BHA, WHA, ANFIS, Rat Swarm Optimization A1gorithm, Delivery Ratio, GWO.

1. INTRODUCTION

The MANET refers to an unstructured wireless network comprising mobile nodes that possess the ability to move in a certain pattern, resulting in a continually evolving topological structure. The MANETs have gained significant attention in various domains, including but not limited to meetings, tactical operations, environmental monitoring, and rescue operations, making them a prominent subject of study [1]. The routes between any two nodes have been constructed with respect to needed basis that represent the brief and subjected to disruption over time for a number of reasons [2], [3]. In transferring data packets across the network, each mobile node in a MANET functions as both a router and a mobile node [4], [5].

The primary concerns associated with the current MANET technology pertain to the security and the routing mechanisms that employed for facilitating communication between mobile nodes. The security of the present MANETs is at risk, as indicated by recent studies. [6], [7]. The primary sources of threat in MANET are hackers or attackers, who often impede the routing of mobile nodes. Nevertheless, a MANET is susceptible to a multitude of internal and external threats due to its inherent lack of centralized administration [8]. The network layer or routing is the primary focus of attacks in MANET, as they are both frequent and detrimental in nature. The three most prominent network layer attacks like Black Hole (BH) Worm Hole (WH) and Gray Hole (GH).The routing path is primarily influenced by the black hole assault [9]. The occurrence of these assaults impedes the process of packet routing, hence resulting in a decrease in network performance.

Due to MANET lack, the centralized architecture and authentication among nodes are susceptible to malicious assaults. To identify and secure the network from these malevolent attempts, IDS are employed. In addition to their evolving topology as well as resource limitations, MANETs are inadequate for traditional IDS. Moreover, the MANET is an array of Mobile Nodes (MNs) in wireless which has ability for communicating with one another with no requirement of centralized administration or fixed infrastructure. Consequently, MANETs developed a desirable technology in numerous applications since they have maintained communications despite the lack of centralized administration or physical infrastructure [10], [11]. But this adaptability also introduces fresh security risks. The basic attack type on MANETs is thought to be the black hole assault. Furthermore, MANETs are not directly protected by the conventional approach to wired or wireless networks using infrastructure. The adoption of IDS is crucial to MANET defence because preventive measures are never sufficient. In identifying the BH attack, a novel method for MANETs featuring an ANFIS and PSO is being presented in this research. Generally, IDS consists of two stages such as data is gathered by Dedicated Sniffers (DSs) as well as CCI has generated, which is then periodically sent to the Super Node (SN). During subsequent stages, the SN utilized a linear regression process in combining the CCIs acquired from various DSs for distinguishing between normal and MNs. The present research provides the detection characterization for various abnormal network circumstances related to the power level as well as node velocity in two dissimilar mobility models such as Gauss Markov (GM) and Random Way Point (RWP) [12]. The RSOA is a cutting-edge program based on swarm intelligence that emulates how rats naturally pursue and combat prey. It was used on a number of optimization issues. The two primary species of rats are black and brown rats. Rats exhibit social intelligence by nature in general. They assist and cooperate with one another on various responsibilities. The primary driving force behind the RSOA is the fact that rats are affectionate creatures that are well-known for their aggressiveness when pursuing and combating prey [13].

The survival of the network and protection against threats to the routing protocol depend on the identification and prevention of routing attacks. The detection systems known as Routing Attack Detection Systems (RADS) [14] are used to keep track of routing attacks. Network layer attacks cannot be prevented by networks routing protocols already in use, such as, DSR, AODV, DSDV, and ZRP [15]. However, the work suggests using ANIFS-RSOA to recognise wormhole and black hole assaults in MANET. Hence, the research concentrated on satisfying cluster and minimizing energy consumption by optimum routing, detecting attacks as well as augmentation of security through security measures. This research objective has concentrated for improving the security of IDS in MANET by clustering the optimization to resolve multifaceted optimization issues and coordinated controllers design using RSOA. To secure from various intruders by combining the uncertainty process capability using fuzzy logic in the ANN learning process. The hybrid ANFIS-RSOA model generates optimal routing as well as attack detection through security measures.

The paper is devised as five sections. In Section 1, the key properties and constraints of MANETs and their attack algorithms are discussed in relation to real-world applications. In Section 2 presents the most modern attack detection methods of related work and a crisp literature survey to identify the problem in detection of different attacks in MANET. Section 3 of this paper introduces the proposed methodology and identifies the challenges associated with the existing Mobile Ad hoc Network (MANET) architecture. Section 4 discussed about optimal routing for security analysis in attack detection process. The application and outcomes of the suggested approach and results are presented in Section 5.

2. RELATED WORK

In the occurrence of such attacks, nodes in the MANET are susceptible to a considerable extent decrease in network performance. The primary value of this research lies in its ability to effectively detect and mitigate malicious nodes that engage in disruptive activities such as wormhole and BH attacks within MANETs [16]. In order to identify and prevent malicious activities such as wormhole and black hole assaults in MANETs, it is imperative to develop mechanisms that can effectively detect and counteract these malicious nodes. The proposed methodology can be employed to mitigate congested traffic by transmitting data packets through a secure route with little latency. A range of criteria, including strength, length, attraction, and robustness, can be utilized to assess the strength of wormholes inside a network. This necessitates the development of a methodology that efficiently safeguards data packets, minimizes energy consumption, and enhances the evaluation of the quality of service provision (QoS). Furthermore, an essential metric for assessing the consequences of an intrusion is the packet delivery ratio. The aforementioned ratio is computed by dividing the quantity of packets that have been successfully delivered by the overall quantity of packets that have been sent.

There have been many research papers and algorithms developed for MANET. Some of these techniques have a substantial communication overhead or require specialized hardware. However, we will highlight studies involving some of the most popular MANET technologies and provide a quick review of all studies that were relevant.

The difficulties of black hole attack in MANETs have been focused by Houda Moudni *et al.* [17]. For the purpose of detecting and preventing attacks from black holes, they used the Fuzzy with PSO algorithm. The hybrid wormhole attack detection (HWAD) technique for MANETs was created by Muhannad Tahboush *et al.* [18]. Their method discovered in-band wormholes by calculating (RTT) round trip time and PDR. The proposed approach involves optimizing the transmission range among nodes to increase hop count and establish out-of-band wormholes more effectively compared to current strategies. Their solution was implemented in the NS-2 platform, and the metrics associated with it were assessed.

The AODV-BS protocols were developed by Prabhakar Reddy *et al.* [19] Black hole attack detection in MANETs. Nagalakshmi.T.J *et al.* [20] investigated a strategy for detecting intrusions using six machine learning algorithms. They constructed the four IDSs without employing feature selection, Instead of depending on familiar ML algorithms such as k-means clustering, decision trees, support vector machines, and random forests. Based on their findings, implementing the feature selection method into IDSs significantly improved their accuracy and detection rates.

The node-based AdaBoost-SVM technique for detecting attacks in MANETs was presented by Hikal Noha A *et al.* [21]. In the first stage, input characteristics were collected and a clustering technique the implementation involved the utilization of the Ad hoc (OMDV) On-Demand Multipath Distance Vector and the LEACH protocol. In addition, their proposed method uses a tuneable threshold value to correctly distinguish between malicious and benign node-dropping behaviour.

Intruder detection systems (IDS) refer to a comprehensive monitoring system and analysing computer system occurrences. An IDS combines complicated approaches with methods for on in the network. The process of gathering data from diverse systems and network sources and subsequently examining it for security vulnerabilities is frequently accomplished through automated means. When it comes to completely protecting network models and locating anomalous behaviours firewalls, access control systems, and other tried-and-true IDS&P methods and encryption fall far short. They investigate for signs of malicious activity and safeguard systems against more complex threats like service denial. In addition, most systems built on such approaches have poor accuracy in detecting threats, large proportion of erroneous positive and negative results, and no flexibility to adapt to evolving malicious activity. Several (DL) Deep Learning Various methodologies have been employed in addressing the issue of intrusion detection with the aim of enhancing detection rates and flexibility, with the ultimate goal of making it simpler for security experts to identify problems in the system. The following table 1 summarises some recent related works.

Table 1 Summary of Related Works

Author & Year	Attack Type	Methodology	Advantage	Disadvantage
Muhannad Tahboush and Mary Agoy [16] & 2021.	Worm Hole Attack	The procedure of hybrid WH Attack Detection is used for identifying mutual in-band WH using K-means Cluster algorithm.	This proposed method has preventing the WH attacks to mutual types such as out-band and in-band. Once evaluation done and compared with hybrid WH attack detection has outperformed while compared to existing network layer attack detection.	Nevertheless, this proposed method has overwhelmed action due to insufficient energy source as well as includes subsequent composite environments.
Houda Moudni et al [18] & 2019	Black Hole Attacks	Proposed hybrid ANFIS-PSO for identifying the attacks in MANET.	PSO has utilized for improving the representation of ANFIS by modifying the membership rules as well as decrease of inaccuracy. Moreover, the proposed method involves high recognition level and generates a low false alarm rate.	Nevertheless, the recommended method is considered and recognized with a less node counts. This doesn’t analyse with several node counts.

Mohanapriya M, Santhosh R [19] & 2021.	Black Hole Attack	This proposed secure method is Dynamic Source Routing (DSR) for securing the MANET from an attack as well as permitting transmission among the nodes while the intruders are existing.	The significant usage of proposed method has consumed less energy consumption when compared with existing methods. Moreover, it recognises the attack short of all performance of computational overhead as well as obtained least packet loss.	In other hand, when the setting is hanged or exceeds vibrant, there is an increase of route request packets that increases the overhead over the dispatch process.
Ngoc T. Luong, Tu T. Vo and Doan Hoang [20] & 2019	Flooding Attack	Flooding Attacks Prevention Routing Protocol (FAPRP) is assist in expanding the AODV procedure.	Based on the simulation output, the recommended FAPRP has realizes sophisticated mischievous recognition level while associated with earlier procedures.	In fixed conditions, the malicious path detection rates have uncertain from the regular nodes. Therefore, the monitor node doesn't accomplish packets beginning from a malicious node until certain remote ahead time.

2.1. Problem Statement

Since MANET is employed more frequently in numerous areas of life that contain more vulnerabilities, which compromise system integrity, security, and accessibility as well as render network resources inaccessible. The resilience and data security of the network environment are seriously threatened by intrusions. Though there are several methods of attack detection with dynamism there are issues of poor energy source as well as leading to subsequent composite environments. Most of the recommended techniques have analysed with less node counts and also need to be analysed with several node counts. Furthermore, when the setting is congested or in extremely vibrant, there will be increase in route request packets that has result in rise of the overheads in the dispatch process. In specific conditions, the malicious path detection rate has uncertain from the normal node. Therefore, it is essential for designing hybrid architecture to prevent unauthorized access as well as improving the performance of the system resources and data. Thus, the research work focuses on hybrid ML method to secure the MANET that assist in monitoring node that avoid packets start from a mischievous node until certain far ahead time.

3. PROPOSED METHODOLOGY FOR DETECTION AND PREVENTION OF ATTACKS IN MANET

The section defines and describes the MANET network layer attacks. In this article, we distinguish between a BHA and a WHA. The BHA is a devastating routing protocol attack that occurs while routes are being calculated. As can be seen in Figure 1(a), during the process of routing, a malevolent node, denoted as M, deceives other nodes inside the network by asserting that it possesses the most effectual path to the intended destination.

In this figure 1(a), the source node, malicious node and destination node is described as B, O and M. While sending any data packets from the node B to node O, meanwhile malicious (BHA or WHA) is occurred in any node, the data packets is dropped because of their malicious node M. Therefore, network security is analyzed because this is an important aspect of MANET. To achieve the network security, attack detection and routing path determination is an important phase of the MANET. In this paper, to achieve the both phases, Enhanced Secure Energy Routing (ESER) protocol is designed for MANETs. The primary focus of this study is on defending MANETs against and identifying network layer assaults (BHA and WHA). Figure 1(c) depicts the methodology's block diagram. The proposed designed protocol is working based on the hybrid technique which is named as the Neuro-fuzzy inference system that can change based on input using the rat-swarm algorithm (ANFIS-RSOA). The suggested protocol detects and prevents assaults in the network, hence resolving the security problem within the framework of the existing system.

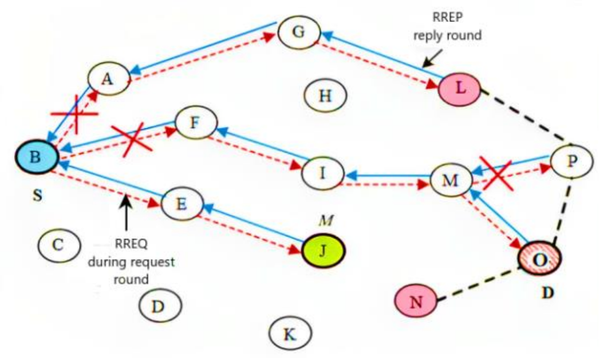

Figure 1(a) Illustration of Behaviour in MANET

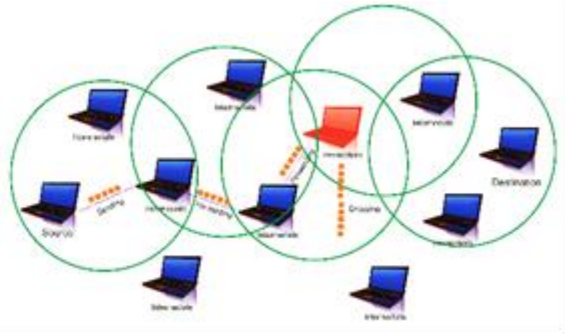

Figure 1(b) Black Hole Atack in MANET

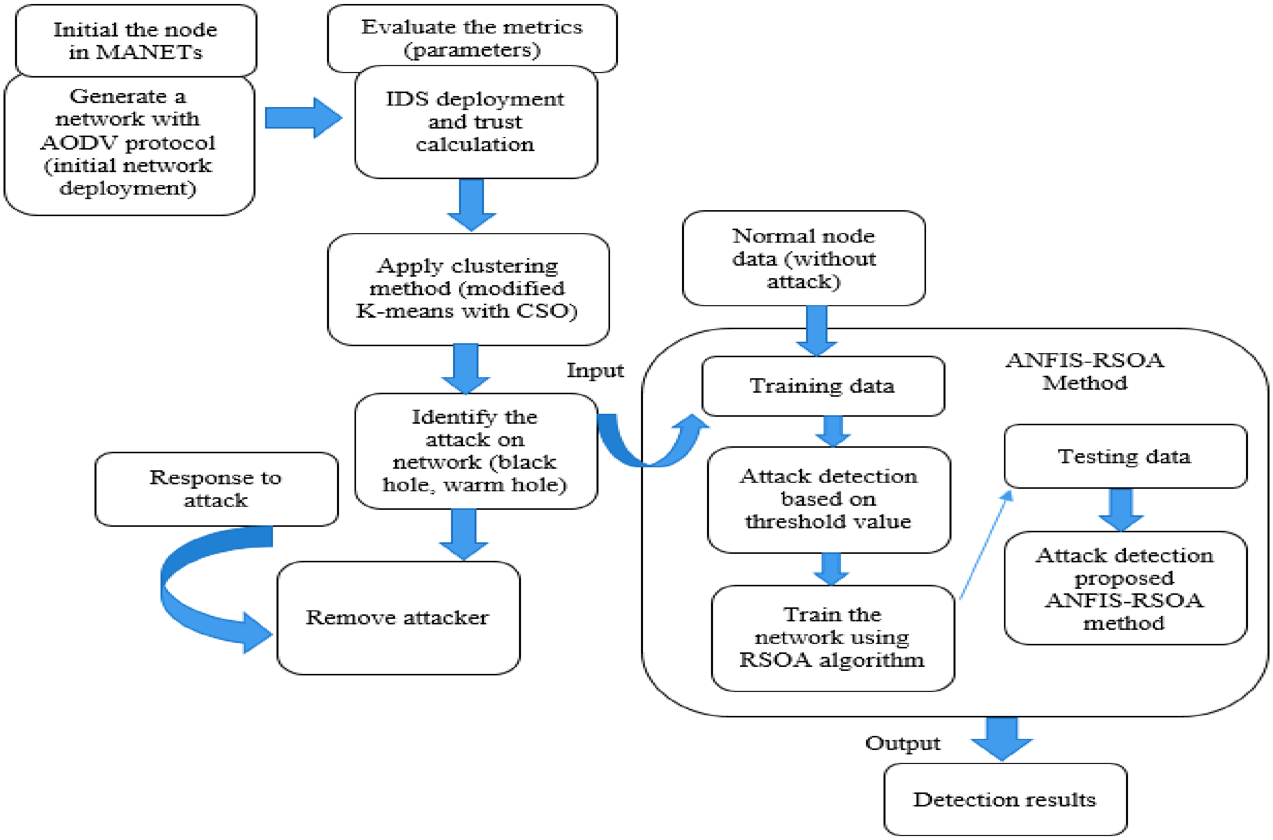
Initial the node in MANETs
Generate a network with AODV protocol (initial network deployment)
Evaluate the metrics (parameters)
IDS deployment and trust calculation
Apply clustering method (modified K-means with CSO)
Identify the attack on network (black hole, warm hole)
Response to attack
Remove attacker
Input
Normal node data (without attack)
ANFIS-RSOA Method
Training data
Attack detection based on threshold value
Train the network using RSOA algorithm
Testing data
Attack detection proposed ANFIS-RSOA method
Output
Detection results

Figure 1(c) Block Diagram

From the Figure 1(a), the routing process of data packets is depicted, showing how a path is established between the malicious node (M) and the source and destination nodes (B, O). When a malicious node acts regularly (i.e., like a non-malicious node) during the routing process in order to evade discovery, but then acts abnormally once joined to a created route, as depicted in Figure 1(b), a black hole attack occurs. It can be specified as the data packets are dropped during the attack period. Therefore, the shortest path routing is needed to avoid these issues. Before that, attack detection is needed and optimal routing is needed to achieve the energy efficient analysis. Regarding that, ANFIS-RSOA method is developed in this paper, the subsequent section provides a comprehensive explanation of the assault detection mechanism.

3.1. Phase A: Attack Detection

A malicious node performs a BHA will employ a reactive routing protocol, shown by the Ad hoc On-Demand Distance Vector (AODV) protocol [23], as a means of promoting itself as the quickest route to the desired node. The malicious node falsely asserts that the route it is using is the most convenient one, without checking its routing table, and then intercepts and deletes all traffic passing through it. To go to node O, node B in Figure 1(a) wants to build a route. For example, node B uses a reactive routing protocol to discover a path to node O; these results in all nodes, including the malicious node M, receiving an RREQ packet. To counteract this, the black hole node is capable of transmitting a falsified RREP packet to the original source of node B, incorporating an elevated destination sequence number. Also, as depicted in the same Figure 1(a), the RREP packet will be sent from either the originating node O or a valid adjacent node with a direct path to the desired node B. As per the prescribed criteria of the reactive routing protocol, the sending node B will select the fastest possible path and the sequence number with the highest destination priority. This means that node B will choose the black hole assault strategy as its attack vector once the Black hole node has successfully acquired the route; it promptly proceeds to eliminate all data packets.

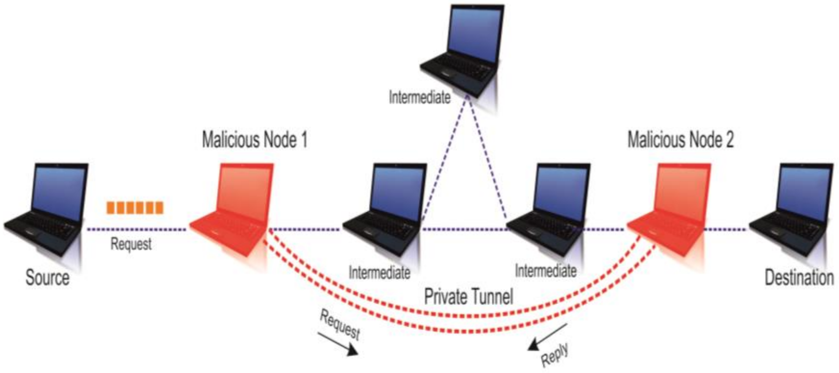

Figure 2 WHA in MANET

The WHA is among the most severe attacks and is seen as a complex issue. The OSI model's layer seven is where it can be started. The routing path and communication link between the Malicious Node 1 and Malicious Node 2 wormhole nodes in Figure 2 is comprised of two malicious nodes. The adversary steals data packets from a particular node in the network, transfers them to another node, and then plays them back to the original node. There are a number of ways to construct the tunnel, some of which fall within the band and some outside of it. For future packet interaction between malicious nodes, the tunnel [22] will be used to determine the path taken by the router to go from point A to point B. Inappropriate nodes can cause packet loss, which can slow down the network or even cause it to crash if critical data isn't delivered in time.

The routing path for an out-of-band attack can be observed as Source, Malicious Node 1, Malicious Node 2 and Destination, as depicted in Figure 2. Consequently, the wormhole node necessitates a transmission mode of greater capacity and an extended range for wireless communication compared to a legitimate node. This allows the wormhole node to create a pathway between two adversarial nodes that are geographically far from one other. Consequently, when the attacker has control over a substantial volume of packets traversing the wormhole tunnel, it will lead to degradation in network performance and the subsequent discarding of packets. In order to determine an appropriate route to the desired location, routing protocols serve as the fundamental framework for the infrastructure of a wireless network. For MANETs, multiple routing protocols have been proposed including proactive and reactive routing techniques. Referring to reference [23], we learn about the AODV protocol, is a widely utilized reactive routing mechanism specifically developed for wireless and mobile ad hoc networks. During the process of transmission, the AODV routing protocol exhibits advantages such as reduced bandwidth consumption, decreased routing overhead, and enhanced convergence speed. In cases where the source node routing database lacks a valid route to the destination, the AODV protocol employs both unicast and broadcast routing mechanisms to determine the appropriate path for communication. Consequently, the source will commence the process of route discovery upon request and transmit a packet to the intended destination through intermediate nodes. In order to establish and sustain the route to the intended destination, the AODV routing protocol employs four distinct types of messages: Route Error (RERR), Route Reply (RREP), Route Request (REQ), and greeting (HELLO) messages. Figure 2 illustrates the process of route discovery in AODV protocols, specifically highlighting the activities of route reply (RREP) and route request (RREQ).

The proposed K-means (PKM) methodology is employed for the purpose of identifying and analysing potentially suspicious and abnormal patterns of user behaviour within network traffic. This approach is specifically designed to facilitate the detection of intrusions inside a network environment. The methodology employs distance as a metric and utilizes the K classes of the dataset as its input. The software then proceeds to compute the average distance between the initial centroid and each of the classes defined by the centroid. The primary aim of the K-Means algorithm is to determine the most suitable centroid value that can be utilized as the threshold for the (PDR) Packet Delivery Ratio. The initial values utilized in the K-Means approaches are derived from a previous study [24] are determined by randomly selecting K items from a range of 0 to 1. Each item chosen represents the average or centre of its cluster. The remaining objects will exhibit similarities and will be allocated to individual clusters. The numbers extracted from the NS-2 trace file, which include coverage statistics and general network details, will serve as input variables for clustering. Subsequently, the algorithm calculates a revised mean or centroid for each cluster and proceeds with iterations to choose the cluster that yields the optimal performance across different initial values. According to the source [25], the range of values for the variable is between 0 and 1. Ultimately, in order to determine the most optimal cluster, it is necessary to compute a novel mean (centroid) value. This value will then serve as the input for the simulator, specifically as the PDR threshold. The utilization of the head cluster is employed for the purpose of ascertaining the cost function, which is afterwards calculated by means of the following equation (1):

$$CH^i = \delta^i * \left(\frac{f^i}{s_t^i}\right) * \omega * N\left(C^i\right) \qquad (1)$$

The optimization algorithms were used to determine the updated consequent and premise parameters in the technique. The CSO algorithm improves the k-means learning process. The following section goes through the CSO procedure in depth.

3.2. Chicken Swarm Optimization Algorithm (CSO)

Meng et al. created the CSO in 2014. This algorithm belongs to the category of modern swarm intelligence-based algorithms. The software emulates the hierarchical structure observed in a chicken swarm, along with its collective food-seeking behaviour. The grouping of the total chicken population into leading rooster, hens, and chicks is determined according to the fitness values of the animals [26].

Chickens with superior food-finding capabilities or fitness are commonly referred to as roosters, whereas those with inferior food-finding capabilities or fitness are denoted as chicks. Chickens displaying intermediate food-finding capabilities or fitness are classified as hens. After each grouping time, the mother–child relationship and hierarchical order are changed. In their search for food, hens follow their group mate rooster, while chicks follow their mother. The algorithm effectively utilizes it. The chickens would engage in scratching behaviour towards the food, leading to an occurrence of intra-flock food aggression.

The method can be divided into two distinct components, namely the start-up phase and the updating phase. In the process of initialization, the population size and many parameters connected to the Community Supported Agriculture (CSO) are determined. These variables include the count of roosters, chicks, hens, and mother hens. The fitness values of the chicken population that was randomly generated were assessed during the start-up process, and a hierarchical order was formed based on these fitness values. Among the group, the largest count is attributed to the hens. Nevertheless, it should be noted that not all hens within the group assume the role of mother hens. Furthermore, the selection of mother hens is conducted randomly from the pool of hens. Lastly, it is seen that the quantity of chicks is lower than that of hens. The present study examines the variations in foraging capabilities among roosters, hens, and chicks [27]. The fitness values of the initial population are modified according to the foraging capabilities exhibited by the different members within the group. The ability of roosters to find food is determined by their fitness level. The following is the formula for updating the position of various types of chickens. The mathematical expression used to calculate the updated position of the rooster is given by the equations (2) and (3):

$$X_{i,j}^{t+1} = \left(1 + Randn(0, \alpha^2)\right) * X_{i,j}^t \qquad (2)$$

$if\ F_i \le F_k, \quad i = 1,2, \dots, k$

$\alpha^2 = 1$, Else

$$\alpha^2 = Exp\left(\frac{(F_k - F_i)}{|F_i| + \omega}\right) \qquad (3)$$

Where, $F_i\ and\ F_k$ is denoted as the fitness value of i^{th} and k^{th} is denoted as randomly selected roosters. $Randn\ (0, \alpha^2)$ is a Gaussian distribution with a zero mean and standard deviation α. ω is referred as small constant. This technique is employed to prevent errors that arise from dividing by zero.

Hens hunt for food with their roosters in their group. Furthermore, chickens have a proclivity for stealing food from other chickens. The hens' current position is calculated by the equations (4), (5) and (6).

$$X_{i,j}^{t+1} = X_{i,j}^t + C_1 * rand * \left(X_{R_1,j}^t - X_{i,j}^t\right) + C_2 * rand * \left(X_{R_2,j}^t - X_{i,j}^t\right) \qquad (4)$$

$$C_1 = Exp\left(\frac{(F_k - F_{R_1})}{|F_i| + \omega}\right) \qquad (5)$$

$$C_2 = Exp\left(F_{R_2} - F_i\right) \qquad (6)$$

Where, $R_1 \in [1, N]$ is a measure of the value of rooster, which is i^{th} hen’s group mate and $R_2 \in [1, N]$ indicates the random selection of a chicken, either a rooster or a hen, from $R_1 \neq R_2$. $rand$ is a made-up number between 0 and 1. The chicks position update is formulated as shown in equation (6a).

$$X_{i,j}^{t+1} = X_{i,j}^{t} + FL * \left(X_{m,j}^{t} - X_{i,j}^{t}\right) \quad (6a)$$

The mother of the i^{th}chick can be located in the coordinates ($X_{m,j}^{t}$). The chick's ability to hunt for food without help from its mother is indicated by the parameterFL. FL is a parameter with a range of [0, 2].In the context of a mobile ad-hoc network (MANET), the suggested algorithm is based on Hybrid Attack Detection (HAD). To avoid conducting wormhole verification in all available nodes, a neighbour ratio threshold (NRT) has been established. The subsequent utilization of the detection algorithm will involve the integration of multiple detection approaches. Several algorithm procedures have been proposed.

Procedure 1:

As outlined in Algorithm 1, the utilization of a method known as the neighbour ratio threshold (NRT) is recommended in order to effectively decrease the quantity of nodes that necessitate exploration.

Procedure 2:

Assess whether the adjacent nodes are located within the transmission range of the source. In the event that the source is beyond the permissible range, it is appropriate to categorize it as an out-of-band wormhole attack, as exemplified in method 2. If the previous condition is not met, then the next step to be taken is step 3.

Procedure 3:

In the event that the adjacent nodes are situated within the range of transmission of the source, using the round trip time based on hop count and PDR, one can identify an in-band attack.

```
Start
for each node $n_i$ in N and its neighbor set $S_i$ in S do
  Let $S_i = | S_i |$ (which is the neighbor number of $n_i$);
  for each node $n_i \in S_i$ do
  $S_j = | S_j |$ (which is the neighbor number of $n_j$);
  Set $a = 0$;
  $a = a + s_j$;
  To find the average neighbor number of $n_i$'s
  neighbors, Then $\overline{si} = \frac{a}{si}$
  To Find the $n_i$'s   neighbor ratio $NRT_i = \frac{si}{\overline{si}}$
  if $NRTi > NRT$ then
  put ni to suspected nodes set A area;
end
```

Algorithm 1 Neighbour Ratio Threshold in CSO

3.3. ANFIS with RSOA for Attack Detection

The ANFIS is a fuzzy inference system that uses an adaptable neural network as a framework. The fusion mechanism and fuzzy logic of neural networks are used in the ANFIS technique. If the neural network product's anticipated input-output data sets are unclear, it can be utilised to build input-output scheduling based on human information. Due to system development, fuzzy logic imposes constraints such as imprecision and uncertainty. The input variable created from the system contribution and output data in the initial fuzzy model is a benefit of fusion technology. For the initial fuzzy model, the neurological system model was successfully applied to meet ANFIS [28] requirements. The computational features of ANFIS are applicable to certain issues. ANFIS's test input-output data records functional boundaries. Fuzzy interface systems are used in the ANFIS model. The adaptive and fixed nodes are displayed individually in the square and circle nodes.

In the ANFIS, Input/output was illustrated by X and Y, where X is represented as $T^e = (x^1, x^2, \ldots\ldots x^n)$ and Y is represented as $\Delta T^e = (y^1, y^2, \ldots\ldots y^n)$. It involves the weight and information procedure of ANFIS, which was applied in the preferred production. Dual fuzzy rules were created and employed the designed ANFIS. The restriction of the ANFIS was established with R^1 and R^2presented below in equations (7) and (8) respectively.

$$R^1\text{: If (X is } x^1\text{) and (Y is } y^1\text{) then } \left(F^1 = r^1X + s^1Y\right) + t^1 \quad (7)$$

$$R^2\text{: If (X is } x^2\text{) and (Y is } y^2\text{) then } \left(F^2 = r^2X + s^2Y\right) + t^2 \quad (8)$$

Where, F^i is denoted as fuzzy region that extended from the output signal in the fuzzy set. $r^i, s^i$and t^i are denoted as the design constraints, which is evaluate the training procedure correspondingly.

From the Figure.3, the input in addition the output of ANFIS can be mentioned as $e(k)$, $\Delta e(k)$, and γ, respectively. The learning cycle of ANFIS is performed on the characterised signals, and it is highly typical to include solidarity weight. Sugeno design can be regarded as as two fluffy presuming principles that rely on an initial request. The ANFIS's instructional concept can take the following form:

$$Rule\ 1: If\ (e(k)_1\ is\ A_1) and\ (\Delta e(k)_1\ is\ B_1)\ then\ (Y_1 = s_1 e(k)_1 + t_1 \Delta e(k)_1 + r_1$$

$$Rule\ 2: If\ (e(k)_2\ is\ A_2) and\ (\Delta e(k)_2\ is\ B_2)\ then\ (Y_2 = s_2 e(k)_2 + t_2 \Delta e(k)_2 + r_2$$

Here, A_i and B_i can be denoted as fuzzy sets. The outcomes of the rectified signal can be (Y_i) in addition it is got from the fuzzy area. The design parameters can be specified as s_i, t_i in addition γ_i, respectively and can be calculated from the training procedure. In a management mechanism, the ANFIS method creates a nonlinear function and a continuous process of nonlinear components. The ANFIS strategy's linear function and non-linear components were created in a continuous process. There are five layers to the ANFIS model. The first layer adds some noise to the inputs. The first layer's output is the input's membership grade.

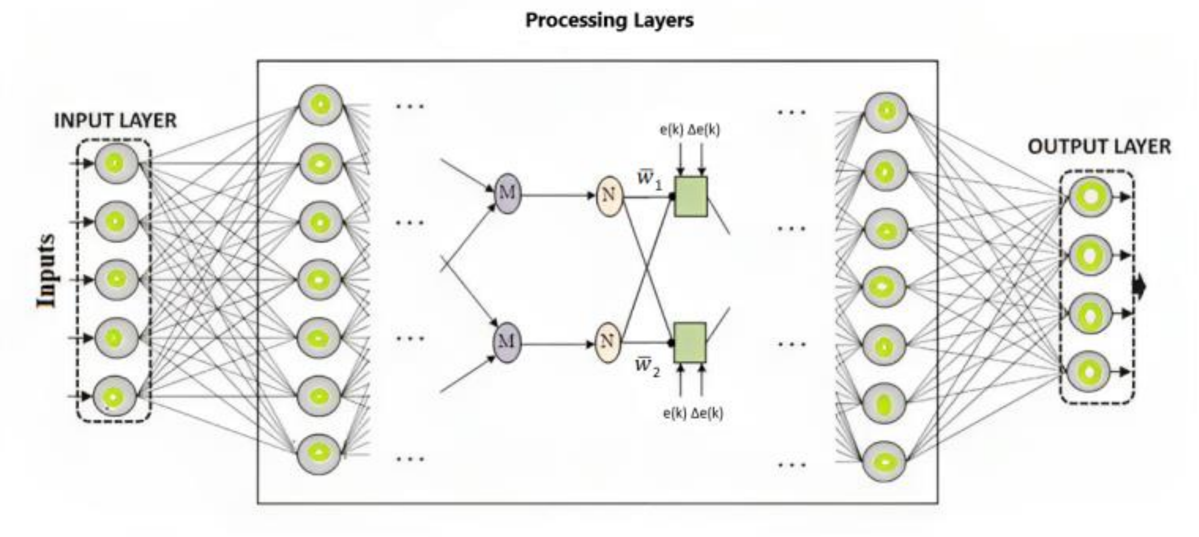

Figure 3 Designs of ANFIS Controller

3.3.1. Layer 1

The input layer of the ANFIS model was examined using neurons. This layer is connected to the external input signal of the layer below. Each node's output was shown using specific equations (9) and (10) respectively,

$$L_i^1(X) = \mu_{x(i)}(X) \quad \text{for } i = 1,2 \qquad (9)$$

$$L_i^1(Y) = \mu_{y(i-2)}(Y) \quad \text{for } i = 3,4 \qquad (10)$$

Where $L_i^1(X)$, $L_i^1(Y)$ are demonstrates the associated grade for X and Y. $\mu_{x(i)}(X)$, $\mu_{y(i-2)}(Y)$ are the fuzzy function that corresponds to the fuzzy set. The bell-shaped distribution is choosing the minimum and maximum values among 0 and 1. The equation (11) gives the bell-shaped function,

$$\mu_{x(i)}(X) = \frac{1}{1+\left|\frac{X-w^i}{u_i}\right|^{2v_i}} \quad i = 1,2,\ldots \quad (11)$$

Where u^i, $v^i$and w^i are the premise parameter which need to discover and create barriers in development.

3.3.2. Layer 2

Each of these layer's nodes resembles a solid circle. Nodes are categorised as M. The effectively evaluated input and output signals in the manners listed below by equation (12).

$$L_i^2(X)(Y) = w^i = \mu_{x(i)}(X) * \mu_{y(i)}(Y) \quad i = 1,2,\ldots \qquad (12)$$

In specific, the input signal connected with the neuronk. w^i is denoted as fuzzy strength of each node.

The beginning process indicates the query in the neuron, and the final process transfers the immediacy input to the weight indicates.

3.3.3. Layer 3

The strengths of the second layer, which are characterized by fuzziness, are normalized within this particular layer. Additionally, it encompasses the clearly defined perimeter of a circular shape. The calculation of the normalised factor involves the summation of weight functions. The equation (13) gives output of the third layer is subject to modification in the following manner.

$$L_i^3 = \overline{w^i} = \frac{w^i}{\sum_i w^i}, i = 1,2,\ldots \qquad (13)$$

3.3.4. Layer 4

This layer's nodes are flexible. It regulates the adaptive relationship between the heating value and the firing value of the termination function, which is inferable from the provided equation. The blur key for the second layer is normalised on that layer. It also includes the solid form of a circle [29]. The calculation of the normalization factor involves the summation of the weight functions. The output of the third layer is handled as shown in the equation (14):

$$L_i^4 = \overline{w^\imath}F^i = \overline{w^\imath}\,(r^i x + s^i y + t^i), i = 1,2, \dots \quad (14)$$

Where r^i, s^i and t^i are a constraint of projected and specified subsequent parameters.

The ANFIS parameters are constructed using both the least-squares and gradient descent methods.

3.3.5. Layer 5

To estimate the aggregate output, a single node was used. The input signal is weighted by the similar synapses of the neuron and calculated by the adder as follows: This layer's nodes are flexible. By adjusting the firing value, it manages how the heat value and finishing process adapt to one another. This result was attained using the equation (15) shown below.

$$L_i^4 = F = \sum_i \overline{w^\imath}F^i = \frac{\sum_i w^i F^i}{\sum_i w^i}, i = 1,2, \dots \qquad (15)$$

Different input operating conditions affect the ANFIS model's efficiency in different ways. The ANFIS model's parameters are updated using the conventional training strategy, which uses a hybrid learning technique that combines gradient descent and least squares approaches. The hybrid learning process' beginning and conclusion steps were unmistakably described. The hybrid learning process involves both a forward pass as well as a backward pass. During the forward pass, the ANFIS model's parameters are revised using the least squares approach. When using the sloping decline approach is also utilised to update the ANFIS premise parameters during the backward pass. A backward pass sends the error to the system for uniform error propagation. The ANFIS exhibition may get burdensome with more indicators. The planned ANFIS regulator looks at ways to increase productivity of the framework as well as measures to cut down on errors.

3.4. Process of the RSOA Algorithm

The RSOA and ANFIS regulators have become accustomed to managing the power within the MANETs, hence enhancing the robustness of the network architecture. Rats are a species of medium-sized rodents characterized by their long tails. Their size and weight might vary, as determined by the RSOA algorithm. The black rat and the brown rat are the two most prevalent species of rats. In the realm of rat taxonomy, it is customary to refer to male rats as "bucks" and their female counterparts as "does." Rats possess inherent social sophistication. The individuals partake in mutual grooming and exhibit various behaviours including as jumping, chasing, tumbling, and boxing [30]. Rats exhibit a social structure characterized by the cohabitation of both male and female individuals within a group, while also displaying territorial behaviour. Rats are recognized for their propensity towards aggression, a characteristic that has been observed to result in the demise of specific animal species.

The pursuit and engagement in combat with prey is a fundamental motivating factor for this job, as indicated by previous research [31]. The user has provided a numerical reference. This study undertakes a mathematical analysis of the chasing and fighting behaviours exhibited by rats, with the objective of constructing the RSO algorithm and conducting optimization.

ANFIS investigates the regulator structure's erroneous boundaries. The RSOA computation is used to define error estimates. The proposed technique's cycle is explained in the steps below.

Step 1: Initialization: Create an initial population of rats. Pi for any integer i from 1 to infinity.

$$\text{Rats} = \begin{bmatrix} X_1^1 & X_1^2 & \dots & X_d^1 \\ X_1^2 & X_1^2 & \dots & X_d^1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ X_1^N & X_1^N & \dots & X_d^N \end{bmatrix} \qquad (16)$$

Each rat has been initialized as in equation (16). At the preliminary iteration, the rats have no initial values; it is concluded that they have hidden their foods at starting process shown by equation (17),

$$\text{memory} = \begin{bmatrix} M_1^1 & M_1^2 & \dots & M_d^1 \\ M_1^2 & M_1^2 & \dots & M_d^1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ M_1^N & M_1^N & \dots & M_d^N \end{bmatrix} \qquad (17)$$

Step 2: The selection of the starting parameters for a Rat Swarm Optimization (RSO) involves determining the values for three variables: A, C, and R.

Step 3: Fitness Function Evaluation: The quality of rat's locations is calculated by introducing the decision variable values in to attack detection and security as shown by equation (18). The fitness function of every rat is computed in this step.

$$F = \min(T_p, C_q, E_i) \qquad (18)$$

Step 4: The best search agent is then explored for the given search domain.

Step 5: The search agents' positions are updated utilizing Equation (19).

Memory updating: The rat memory is revised using the formula below,

$$M^{t+1} = \begin{cases} X_a^{t+1} & f(X_a^{t+1}) \text{ is better than } f(M_a^t) \\ M_a^t & \text{Otherwise} \end{cases} \quad (19)$$

Where f(.) can be represented as the objective function value of the system; In the event that the fitness function parameter associated with the new position of a rat surpasses the fitness function parameter associated with the rat's memory location, the rat proceeds to update its memory by adopting the optimal location.

Step 6: Verify that no search agent crosses the search space's outer limit before making any necessary changes. If an alternative option surpassing the previous optimal solution exists, the fitness value of the search agent should be recalculated, and subsequently, the vector Pr needs to be updated accordingly.

Step 7: If the halting requirements are met, stop the algorithm. If not, go back to Step 5.

Step 8: The best ideal solution should be returned. Administrators can be characterised by their publishing power, compulsions, and problem making decisions. Analyze the applicability of the new position: Due to the rat's new position, the reliability has been destroyed. Rats will shift positions when their new situation is feasible. Until an agreement can be made, the rat will remain in its current state and won't switch to the novel state of production.

Step 9: Check the end condition: The aforementioned improvements are being redesigned till they acquire greater significance. The arrangement of executives and the severity of the issue at the last stage of meeting the criteria delay the memory's optimal condition in relation to the target value. The proposed methodology is assessed utilizing the NS2 Simulator, and section 4 presents the performance study's findings. Prior to that, the next step is examined and a thorough explanation is given.

4. PHASE B: OPTIMAL ROUTING FOR SECURITY ANALYSIS

The suggested MANET routing protocol aims to ascertain the optimal path based on varying demand conditions. The data packet is not sent regularly in this protocol because the destination checks amount of private keys that will be made available to that node. Data packets at both ends are encrypted using the suggested protocol. After the target node has been authenticated, the sender's data packets are secured using the suggested technique. The shortest path with the least amount of time for sending messages from the sender to the receiver is used in the optimum routing procedure. After that, we apply the Rat Swarm Optimization Algorithm to fine-tune our routing procedure.

The ideal routing plan is obtained for security purposes, and the attacker node is located. The suggested routing strategy incorporates the utilization of routing progress once authentication is accomplished. When one node has to initiate contact with another, it must first authenticate using the suggested algorithm as detailed in 3.2. It then sent an RREQ redirect the inquiry to request a communication node. Each node possesses a routing table that encompasses essential data, including time, lifetime, goal sequence number, original source sequence number, final identification, and original identity. To approve the path, the arrangement number, also known as the Destination Sequence Number (DSN), is checked after arriving at a node to see if it is more noticeable than the counted succession preserved. The node then sends an RREP to the beginning node, with the data on the opposite channel. When the route is put up, it is timed to avoid processing all of the packets; the process terminates with the arrival of a packet.

The suggested protocol is made up of several phases. The Adaptive Rat Swarm Optimization with Cuckoo Search Algorithm approach is used to authenticate the node in the first step. The proposed approach is used to identify the malicious node that was removed from MANETs unexpectedly. The BHA and WHA attack nodes, as well as a corrupted RSU, are discovered, causing the system's performance to collapse. As a result, during the communication process, the rogue node was removed from the network. The data packet is secured and transmitted to all MANET neighbour nodes in the second stage. In the third stage, we make sure the broadcast packet made it into the loop. Finally, once the neighbour node has been verified as safe, the secret key will be given to it. Consequently, the validation process is performed on the packet's request and answer types, ensuring their accuracy and integrity, after which the packet is transmitted. The reputation associated with neighbours' nodes should be computed by the nodes. There are two sub-phases to this computation.

4.1. Calculation of the Node's Local Reputation

Every each node will possess the capability to independently compute the repute of the adjacent nodes. The utilization of retransmission is employed during the transmission of the message by the local node. The process encompasses various elements, including the non-delivery of messages by neighbouring nodes, the presence of defective packets, unaddressed requests, and delays in transmission.

4.2. Calculation of the Node's Final Reputation

The methodology for calculating the forwarding nodes of the RREQ packet stays consistent. The ultimate repute of the node is determined by a technique that incorporates the value of WILLING and introduces a new element to determine the selection. The implementation of the proposed technique leads to an enhancement in security measures. By selecting the most optimal trust node within the framework, the suggested technique improves security. To choose the best trust node, the proposed approach is employed. Two separate trust measures, such as transmission delay and the goal function is the number of packets successfully transmitted from a cluster leader or source node. The equation (20) gives the primary purpose of safeguards is to ensure:

$$Se^{M} = \frac{F^{1}}{F^{2}} \qquad (20)$$

Where $F^{1}$is a two-parameter function characterized by the node's remaining energy and the amount of packets it has transmitted. The amount of energy still present in a node after taking into account one full communication round is referred to as the remaining energy. F^1 is a function that also calculates the quantity of packets sent by the communication process through the node given by equation (21).

$$F^{1} = N^{RE} \times N^{PF} \qquad (21)$$

The term N^{PF} means the total amount of data that has been transmitted. The term $N^{RE}$is described as refers to the residual node energy. Similarly, F^{2} the function is characterized by three components, transmission delay, namely node density, and average cluster distance. The typical separation between clusters (N^{CD}) refers to the mean distance between a node and all other nodes within the same cluster. The formulation for calculating the average distance between clusters is given as equation (22) :

$$N^{cd}(O) = \frac{\sum_{I=1}^{S-1}(Distance(N^{O},N^{I})}{S} \qquad (22)$$

The variable "S" represents the aggregate quantity of nodes within a cluster. N, $N^{cd}(O)$, whereas O (O stands for the average distance of a node in a cluster N to all other nodes in the cluster N).In the given equation, the variable $Distance(N^{O}, N^{I})$ represents the distance between node O and the other nodes inside cluster N. In order to do computations for a given function F^{2} , three essential components must be taken into consideration. These N^{CD} components include the delay of data packet transmission, which is determined according to the relative speed of each node's transmission to the size of data packets in the link(N^{TD}), as well as the factor of node density, which stands for the total number of cluster nodes (N^{ND}). The function F^{2} is defined by the equation (23) given here.

$$F^{2} = N^{CD} \times N^{ND} \times N^{TD} \qquad (23)$$

The third reason why we take precautions is determined by the computation of the third equation, which is expressed in equation (24):

$$Fitness\ (3) = Se^{M} = \frac{N^{RE} \times N^{PF}}{N^{CD} \times N^{ND} \times N^{TD}} \qquad (24)$$

The objective function presented below pertains to the augmentation of security measures within the system. The security mechanisms implemented on each node inside the clustered system have been augmented, as indicated by equation (18). The suggested approach is intended to address the goals of energy efficiency, optimal routing, clustering, and security metrics. The RSOA algorithm is utilised for that process, and phase A of the analysis discusses the algorithm in full.

Finally, the suggested RSOA is used to compute the MANET optimal results in relation to the fitness function. The ideal system is able to shorten transmission times, use less energy, and improve security. The outcomes section examines how the developed technique is presented. To confirm the effectiveness of the established technique, performance evaluation is crucial. The section below presents the simulation results for the created approach.

5. RESULTS AND DISCUSSIONS

The environment of MATLAB R2018A was used in the simulation whereas both optimization and detection approaches have been employed to assess the MANET performance. By looking at the quantitative outcomes of the different metrics utilized to assess the performance of subsequent protocols. This is possible to ascertain the current performance with the suggested programs in MANET. The IEEE 802.11 standard makes use of MAC layer protocol in the Network Simulator (NS2) is used to implement the suggested ANFIS-RSOA model. The proposed ANFIS-RSOA model is evaluated using NS2 simulator in which the setup of implementation parameter shown in Table 2. Moreover, this can be determined through time taken by data packets for propagating from source to region in MANET. Hence, these evaluation metrics involves possible delays caused by the criticality during route detection, MAC return delays, distribution and transmission times, throughput, jitter, packet drop and end delays performance is compared with existing IDS methods such as GWO, WAO and ANFIS-PSO.

Table 2 Parameters for Implementation

S. No	Parameter Description	Parameter Value
1	Channel	Wireless channel
2	MAC	802_11
3	Antenna	Omni Antenna
4	Propagation	Two ray round
5	Antenna	Omni Antenna
6	Dimension of X	1000 m
7	Dimension of Y	1000 m
8	Simulation time	100 s

9	Initial energy	10
10	Maximum packets	2500
11	Initial receive power	0.395
12	Initial transmit power	0.660
13	Initialization of nodes	100 nos
14	Initial idle power	0.035

This proposed session has illustrated the ANFIS-RSOA model utilized trusted nodes, trusted cluster head and trusted gateway for forwarding the data packets from source to destination shown in figure 4(a) and 4(b). The Figure 4(a) shows the initiation of nodes and Figure 4(b) illustrates the simulators that employed when software models network's behaviour by monitoring node behaviour and its services or by applying logical notations or formulae. When a node joins a cluster once it has formed, it sends a join message to the cluster head and a leave message when it exits the current cluster and joins a new one shown in Figure 5(a). There are four input parameters namely degree, buffer duration, mobility, and modification in energy consumption throughout a range of interval intervals to generate clusters. Based on ANFIS-RSOA, the Cluster Head (CH) has been chosen from each cluster. The CH is chosen by each cluster from among its nodes and the routing operation is handled based on the node type is shown in Figure 5(b). Through gateway nodes, the CH has the capacity to communicate with one another. A gateway is a different kind of cluster node that is characterized as a node that has two or more cluster heads as neighbours. Because route requests are only delivered between cluster heads and do not need to traverse the entire network, the clustered approach results in minimal traffic. Security measures are implemented in order to assess the detection of attacks. The identification of the attack node within the MANET architecture has been conducted through the analysis of security measures. With the help of the suggested algorithm, the cluster formation is created. The suggested algorithm is used to build clusters by choosing CHs. With the aid of a hybrid algorithm, the best routing is accomplished while minimising the architecture's additional energy usage.

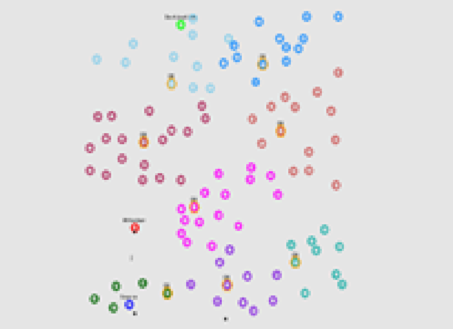

Figure 4(a) Initialization of Nodes

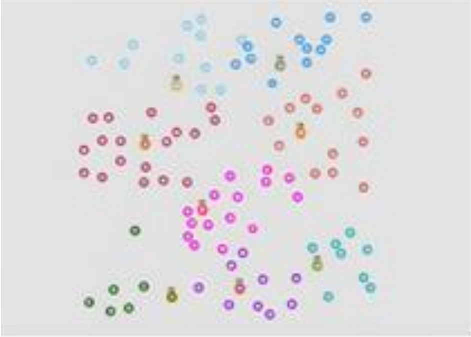

Figure 4(b) Attacks Detection

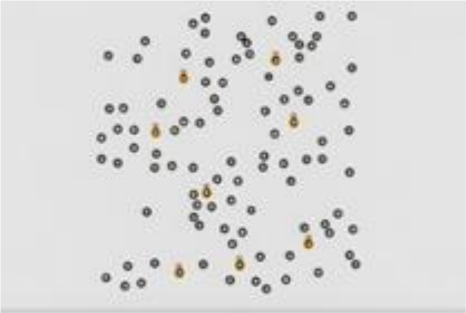

Figure 5(a) Analysis of Cluster Formation

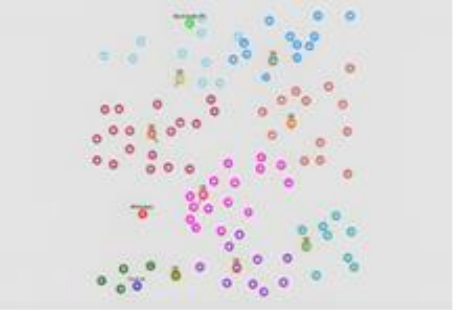

Figure 5(b) Analysis of Head Selection

The figure 6 illustrates the delay of the IDS model with respect to the number of nodes involves, as the number of node increases with respect to the delay increases. The MANET performance of model in energy consumption is by minimizing the delay metrics in proposed ANFIS-RSOA model and the node interval is 10. The delay is very low in ANFIS-RSOA model while compared to other existing model like WOA, GWO and ANFIS-PSO. The delay of ANFIS-RSOA is 3 at node 20 and 11 at node 100 which is comparatively lower than other existing IDS model. The system's delay has been decreased by the suggested algorithm. The GWO algorithm achieves a maximum delay of 15.5 and a minimum delay of 6. The minimum delay for the WOA algorithm is five, and the maximum delay is twelve. Conclusion is that the suggested strategy achieves results with little delay and is regarded as the optimal choice.

Figure 7 illustrates the PDR in MANET, the performance of detecting the intruder and accessing the source-destination route with numerous data is determined through percentage. The packet delivery ratio is high in proposed ANFIS-RSOA while compared to existing IDS model. The delivery ratio decreases with number of modes increase. The system's delivery ratio must be kept at a high level to be rated the best system when analysed. The percentage of times when the suggested system is 0.78 at the lowest rate and 0.93 at the highest rate. The system's delivery ratio has been decreased by the suggested algorithm. The minimum and maximum delivery ratios for the GWO algorithm are 0.72 and 0.85, respectively.

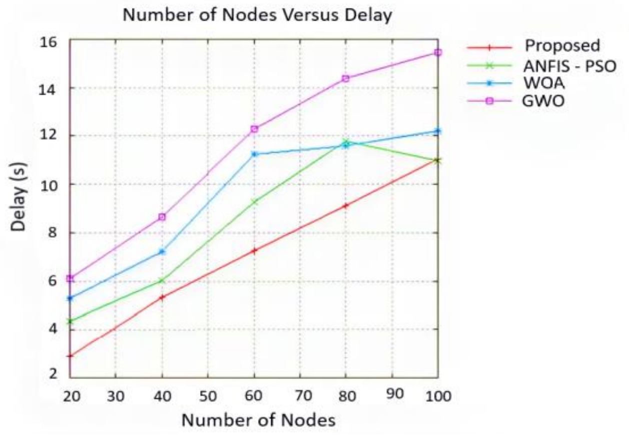

Figure 6 Analysis of Delay

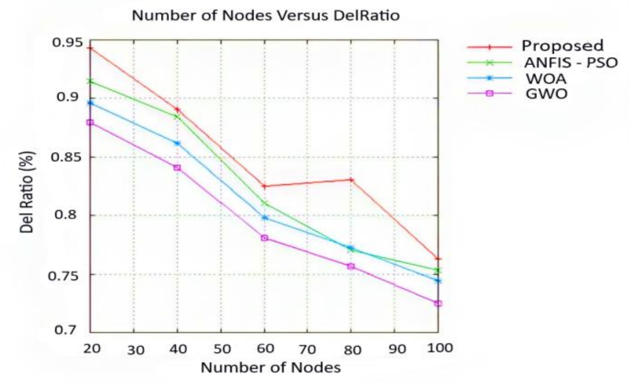

Figure 7 Analysis of Delivery Ratio

Figure 8 illustrates the intruder intense with drop performance statistic. The proposed ANFIS-RSOA model has very less drop while compared to the existing IDS model. The proposed system's drop exhibits a lower bound of 100 and an upper bound of 600 in which the drop is lessened in ANFIS-RSOA model. The lowest and maximum drops for the GWO algorithm are 200 and 2250, respectively. The smallest drop for related to the PSO algorithm is 150, also the highest drop is 1700. The minimum and maximum drop using the WOA is 700. The recommended technique is successful despite having a rather modest decline, making it the best answer, according to the conclusion. The delivery ratio of the various nodes with different methods are tested and tabulated in the table 3.

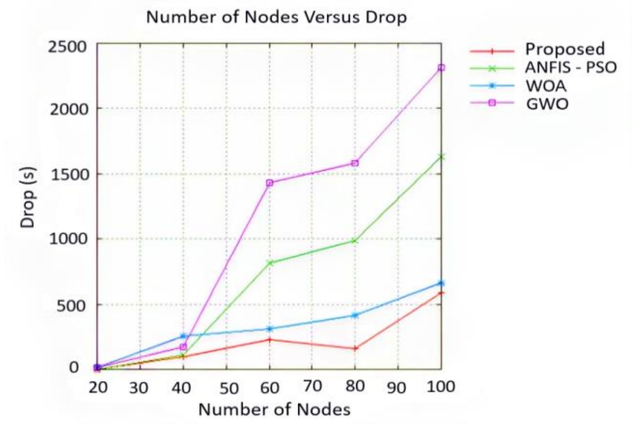

Figure 8 Analysis of Drop

Table 3 Delivery Ratio on Different Nodes with Various Methods

	Delivery ratio (%)				
	Number of nodes				
Methods	20	40	60	80	100
Proposed ANFIS-RSOA	0.93	0.87	0.83	0.84	0.76
ANFIS-PSO	0.92	0.86	0.81	0.77	0.752
WOA	0.89	0.87	0.78	0.77	0.748
GWO	0.87	0.84	0.77	0.73	0.72

In Table 4, the average analysis of the delivery ratio, drops and throughput are analysed. As a result of our investigation, it can be concluded that the proposed strategy has yielded superior outcomes when compared to the existing methods. The same is true for other conventional methods like PSO and WOA.

Table 4 Average Analysis of Drops and Delivery Ratio

Methods	Delivery ratio (%)	Drops (s)	Throughput (kbps)
Proposed ANFIS-RSOA	0.8461	222	48400
ANFIS-PSO	0.8224	702.4	41700
WOA	0.8116	362.8	38800
GWO	0.7861	1103	35400

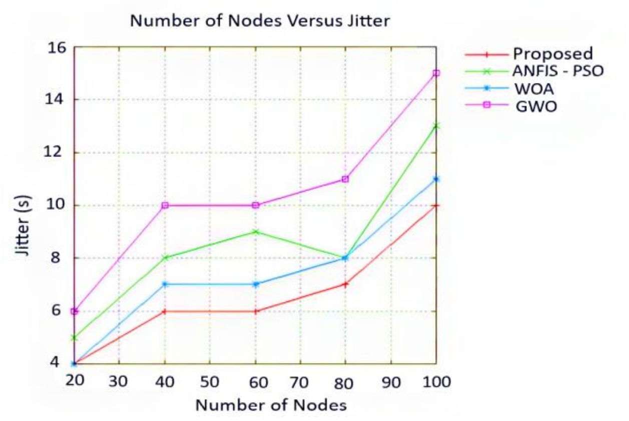

Figure 9(a) Analysis of Jitter

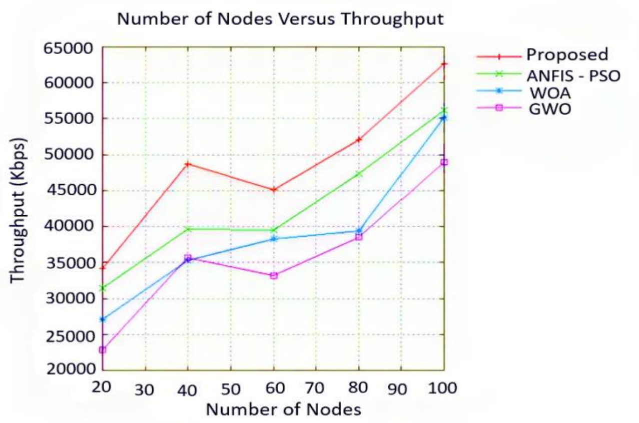

Figure 9(b) Analysis of Throughput

Figure 9(a) illustrates the jitter of the model in the MANET, it determine the packet variance delay of the model in the MANET. The proposed ANFIS-RSOA has low jitter that represents the less time consumption in reaching the destination node from source. As the number of node increases the jitter will increase for all IDS models but in certain nodes it may decreases. The proposed ANFIS-RSOA consumes 10ms for maximum node as 100 but in the case of existing node like WOA, ANFIS-PSO and GWO are 11ms, 13ms and 15ms respectively. One of the essential metrics in determining the performance of the MANET is throughput which is measured through kbps as shown in Figure 9(b). The amount of packets delivered per second is also mentioned as throughput in which proposed ANFIS-RSOA has high throughput value from node 20 to 100 as 35000kbps to 62500kbps and comparatively high with other existing IDS model that consumes maximum value in node 100 for ANFIS-PSO, WOA and GWO are 56000 kbps, 55000kbps and 49000kbps respectively. The method that has been proposed while compared to the current methods, yields the best throughput and overall good results determines the high secured and less energy consumption using ANFIS-RSOA.

6. CONCLUSION

In this research, the ANFIS-RSOA approach is used to detect and avoid wormhole and predatory black holes in MANETs. The input parameters of the method are obtained from a database associated with MANET that obtained by creating a neighbour table that records the activity of all neighbouring nodes. The proposed ANFIS-RSOA incorporates various mechanisms to boost its performance, including clustering formation, energy saving through effective routing, and security enhancement via the implementation of security measures are calculated to meet the aforementioned objective functions. Using the suggested ANFIS-RSOA technique, attack detection and security are accomplished along with optimum routing which minimizes MANET's energy usage. The suggested method has been tested employing the NS2 modeller, and compared with current contemporary approaches via PSO, WOA, and GWO for performance. The results of testing reveal that the proposed methodology approach has a satisfactory level of detection rate and jitter rate. The performance measures encompass delay, drop, throughput, energy utilization, delivery ratio, and jitter. The simulation results demonstrate that the proposed technique exhibits superior performance compared to existing approaches in terms of delivery ratio, latency, and drop rate. In the future, the identification and mitigation of various security breaches in MANETs could be accomplished by the utilization of diverse algorithms. Additionally, a routing method based on multipath routing protocols will be developed. To optimize security, a cryptographic method will be implemented within the system.

REFERENCES

[1] Zulfiqar Ali Zardari, Kamran Ali Memon, Reehan Ali Shah, Sanaullah Dehraj, Iftikhar Ahmed, “A lightweight technique for detection and prevention of wormhole attack in MANET”, EAI Endorsed Transactions, Scalable Information Systems, Vol.8, No. 29, 2021

[2] Safaa LAQTIB, Khalid El YASSINI and Moulay Lahcen HASNAOUI, “A Deep Learning Methods for Intrusion Detection Systems based Machine Learning in MANET”, IJECE, Vol 10, No. 3, June 2020, pp 2701-2709

[3] Alka Chaudhary, V.N. Tiwari and Anil Kumar, “Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks”, Int. J. Soft Computing and Networking, Vol. 1, No. 1, 2016 – 17

[4] Udaya Kumar Addanki, B. Hemantha Kumar, “Enhancement OLSR Routing Protocol using Particle Swarm Optimization (PSO) and Genrtic Algorithm (GA) in MANETS”, IJCSNS International Journal of Computer Science and Network Security, VOL.22, No.4, April 2022

[5] Kumaravel, A., Chandrasekaran, M. Performance analysis of malicious node detection in MANET using ANFIS classification approach. Cluster Comput 22 (Suppl 6), 13445–13452 (2019). https://doi.org/10.1007/s10586-018-1955-z

[6] Mukul Shukla, Brijendra Kumar Joshi, Upendra Singh, “Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET”, Wireless Personal Communications (2021) 121:503–526

[7] Shalini Jain, Satbir Jain, “Detection and prevention of wormhole attack in mobile adhoc networks”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010

[8] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, 2013, 5, 64-72.

[9] K Srinivas, V Harsha Shastri, Vinay Kumar Nassa, Gudapati Syam Prasad and Prathipati Ratna Kumar, "Discernment and Diminution of Black Hole Attack in Mobile Ad-Hoc Network using Artificial Intelligence", 2021 doi:10.1088/1742-6596/2040/1/012037

[10] Ausaf Umar Khan, Milind Madhukar Mushrif, Manish Devendra Chawhan, Bhumika Neole, "Performance Analysis of Adhoc On-demand Distance Vector Protocol under the influence of black-Hole, Gray-Hole and Worm-Hole Attacks in Mobile Adhoc Network", Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021)

[11] Moudni, H., Er-rouidi, M., Mouncif, H., & Hadadi, B. E. (2019). Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET. Procedia Computer Science, 151, 1176–1181. doi:10.1016/j.procs.2019.04.168

[12] Amouri, A.; Alaparthy, V.T.; Morgera, S.D. A Machine Learning Based Intrusion Detection System for Mobile Internet of Things. Sensors 2020, 20, 461. https://doi.org/10.3390/s20020461

[13] G. Dhiman, M. Garg, A. Nagar, V. Kumar and M. Dehghani, "A Novel Algorithm for Global Optimization: Rat Swarm Optimizer," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 8, pp. 8457–8482, 2021.

[14] John Felix Charles Joseph, Amitabha Das , Bu-Sung Lee , Boon-Chong Seet, "CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS", Computer Networks 54 (2010) 1126–1141

[15] Aniruddha Bhattacharyya Arnab Banerjee Dipayan Bose, "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques", april 20, 2022

[16] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", 2014 DoI:10.1145/986537.986560.

[17] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif and Benachir ElHadadi, "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET", Procedia Computer Science, Vol. 151, pp. 1176-1181, 2019

[18] Muhannad Tahboush and Mary Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)", IEEE Access, Vol.9, 2021

[19] Prabhakar Reddy, Bhaskar Reddy, Dhananjaya, "The AODV routing protocol with built-in security to counter blackhole attack in MANET", Materials Today: Proceedings, Vol. 50, Part 5, pp. 1152-1158, 2022

[20] T.J.Nagalakshmi, A.K.Gnanasekar, G.Ramkumara A.Sabarivani, "Machine learning models to detect the blackhole attack in wireless adhoc network", Materials Today: Proceedings, Vol. 47, Part 1, 2021, pp. 235-239

[21] Hikal Noha A., Shams Mahmoud Y., Salem Hanaac, Eid Marwa M., "Detection of black-hole attacks in MANET using adaboost support vector machine", Journal of Intelligent & Fuzzy Systems, vol. 41, no. 1, pp. 669-682, 2021

[22] Van-Hau Nguyen, Vi Hoai Nam, Linh Manh Dao, Quy Vu Khanh, "An Improved Agent-Based AODV Routing Protocol for MANET", June 2021Industrial Networks and Intelligent Systems 8(27):1-8, 2021

[23] Abdul Majid Soomro, Mohd Farhan Bin Fudzee, Muzamil Hussain and 3Hafiz Muhammad Saim, "A Hybrid Routing Approach Comparison with AODV Protocol Regarding Speed for Disaster Management in MANET", Journal of Computer Science, Vol. 18, No.3, pp. 204-213, 2022.

[24] Xiaojuan Ran, Xiangbing Zhou , Mu Lei , Worawit Tepsan and Wu Deng , "A Novel K-Means Clustering Algorithm with a Noise Algorithm for Capturing Urban Hotspots", Appl. Sci., 11, 2021.

[25] Fouad H. Awad and Murtadha M. Hamad, "Improved k-Means Clustering Algorithm for Big Data Based on Distributed Smartphone Neural Engine Processor", Electronics 2022, 11, 2022

[26] Leticia Amador-Angulo, Oscar Castillo, Cinthia Peraza and Patricia Ochoa, "An Efficient Chicken Search Optimization Algorithm for the Optimal Design of Fuzzy Controllers", 2021.

[27] Zhenwu Wang, Chao Qin, Benting Wan, William Wei Song, and Guoqiang Yang, " An Adaptive Fuzzy Chicken Swarm Optimization Algorithm", Mathematical Problems in Engineering, 2021.

[28] Ramesh Kumar Selvaraju, Ganapathy Somaskandan, "ACS algorithm tuned ANFIS-based controller for LFC in deregulated environment", Journal of applied research and technology, Vol.15, No.2, 2017

[29] Issam Griche, Messalti Sabir, Kamel Saoudi, Yaakoub Mohamed Touafek, "A New Adaptive Neuro-Fuzzy Inference System (ANFIS) and PI Controller to Voltage Regulation of Power System Equipped by Wind Turbine", European Journal of Electrical Engineering 21(2):149-155, 2019.

[30] Ali Toolabi Moghadam , Srete Nikolovski, Mahdiyeh Eslami, Shima Rashidi , Morteza Aghahadi and Behdad Arandian , "Adaptive Rat Swarm Optimization for Optimum Tuning of SVC and PSS in a Power System", International Transactions on Electrical Energy Systems / 2022.

[31] Gaurav Dhiman, Meenakshi Garg, Atulya Nagar, Vijay Kumar and Mohammad Dehghani, "A novel algorithm for global optimization: Rat Swarm Optimizer", Journal of Ambient Intelligence and Humanized Computing, Vol. 12, pp. 8457–8482, 2021.

Authors

Sivanesan Narayanan received **B.E** Degree in Computer Science and Engineering from Bharath Institute of Science and Technology, Chennai Affiliated to University of Madras, Chennai, Tamilnadu in 2001. **M.E** degree in Computer Science and Engineering from Jerusalem College of Engineering, Chennai Affiliated to Anna University, Chennai, Tamilnadu in 2006. He is currently a research scholar in the Department of Computer Science and Engineering at Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India. He has more than one and a half decades of teaching experience. His research interest includes machine learning, mobile ad-hoc network and cryptography.

Dr A. Rajesh received the M.Tech. in Computer science and Engineering, from the VIT University, Vellore, Tamilnadu, India (2004) and his Ph.D. from Anna University, Chennai, Tamilnadu, India(2017). He is presently the Associate Professor of Computer Science Engineering at the School of Engineering of VISTAS University, Chennai, Tamilnadu, India, where he has established an advanced research Virtual Reality laboratory, emphasizing AR-VR visual hybrid racking approach and the guiding part of a reliable indoor navigation requests for 3D model of the environment. His research interest includes technology and applications of Machine Learning, AR-VR Technology and Trusted Network telecommunication.

Dr. K. S. Archana received her Master of Engineering degree in Department of Computer Science and Engineering from Sri Krishna Engineering College, Chennai, in 2010. She received her Ph.D. degree in Department of Computer Science and Engineering from Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, in 2020. She is currently working as an Assistant Professor in Department of Data science and Business systems, SRM Institute of Science and Technology, Kattakulathur, Chengalpattu District- India - 603203.She has 14 years of Teaching and Research experience which has helped her to gain immense knowledge in myriad fields of Computer Science and Engineering. She has published more than twenty papers in reputed journals and conferences. Her main research interest includes Image Processing, Machine Learning and Networking.

How to cite this article:

Sivanesan N, Rajesh A, K. S. Archana, “ANFIS-RSOA Approach for Detecting and Preventing Network Layer Attacks in MANET”, International Journal of Computer Networks and Applications (IJCNA), 10(6), PP: 976-992, 2023, DOI: 10.22247/ijcna/2023/223693.