Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

# Watchdog malicious node detection and isolation using deep learning for secured communication in MANET

Narmadha A. S., Maheswari S. & Deepa S. N.

**To cite this article:** Narmadha A. S., Maheswari S. & Deepa S. N. (2023) Watchdog malicious node detection and isolation using deep learning for secured communication in MANET, Automatika, 64:4, 996-1009, DOI: 10.1080/00051144.2023.2241766

**To link to this article:** https://doi.org/10.1080/00051144.2023.2241766



Published online: 01 Aug 2023.

AUTOMATIKA
2023, VOL. 64, NO. 4, 996–1009
https://doi.org/10.1080/00051144.2023.2241766



# Watchdog malicious node detection and isolation using deep learning for secured communication in MANET

A. S. Narmadha[a], S. Maheswari[b] and S. N. Deepa[c]

[a]Department of ECE, Hindusthan Institute of technology, Coimbatore, India; [b]Department of EEE, Kongu Engineering College, Erode, India; [c]Department of Electrical Engineering, National Institute of Technology, Arunachal Pradesh, Jote, India

**ABSTRACT**

Mobile Ad-hoc Networks (MANETs) are wireless networks formed dynamically by connecting or leaving nodes to and from the network without any fixed infrastructure. These categories of wireless networks are susceptible to different attacks based on their dynamic topological structure. Due to this, security is a primary constraint in MANETs to preserve communication between mobile nodes. A Deep Neural Learned Projective Pursuit Regression-based Watchdog Malicious Node Detection and Isolation (DNLPPR-WMNDI) technique is proposed and modelled in this paper to improve the security feature of MANETs. The newly proposed DNLPPR-WMNDI technique initially selects the neighbouring nodes by applying the projection pursuit regression function. In multicasting, the route paths are established through the intermediate node with the help of control commands named RREQ and RREP. After then, Watchdog Malicious Node Detection and Isolation (WMNDI) technique is applied to detect malicious nodes based on the data packet forwarding time. Basically, a malicious node is affected by a node isolation attack. For better communication, a malicious node is isolated from the network and multicast routing is carried out by selecting the next neighbouring node and this improves the communication security. Simulation is done for the developed technique based on different performance metrics.

**ARTICLE HISTORY**
Received 24 May 2023
Accepted 22 July 2023

**KEYWORDS**
MANET; secure communication; deep neural network learning; projection pursuit regression function; watchdog malicious node detection; isolation

## 1. Introduction

MANETs are mobile ad-hoc networks that possess a routable networking environment over the top of the link layer ad-hoc network. These MANETs comprise a set of mobile nodes that are connected in a wireless form within a self-configured network model deprived of a static structural design. Figure 1 shows the basic MANET architecture. The main demanding issue for the MANET is to equip every device to continuously preserve the information needed to correctly route traffic. MANET nodes are capable of moving freely in a random manner as and when the network topology gets changed repeatedly. All nodes behave as a router as they forward traffic to other specified nodes in the network. MANETs adopt dynamic topology to form unidirectional and bi-directional connections. MANETs are used for different real-time applications like emergency operations, rescue operations, military applications, flexible, low-cost, and dynamic infrastructure, road-safety operations, air/ land/navy-based defense operations, weapon handling and so on. Security plays a vital role to improve the communication between mobile nodes in MANETs.

A different routing protocol is vital for MANETs for finding multi-hop routes to transmit data packets from one node to another node. The MANET routing protocol has mainly divided into three types namely proactive and reactive routing and hybrid routing. Proactive routing is named table-driven routing in which the routing table comprises the routing information of every node in the network. The reactive routing protocol has On-demand protocols. These routing protocols are available in MANET such as Dynamic Source Routing (DSR), and Ad hoc on-demand Distance Vector (AODV). A hybrid routing protocol is to perform the concept of integrating nodes into groups as well as permits diverse services to nodes in a group.

Mobile Adhoc Networks are vulnerable to numerous security attacks. The security attacks in MANET are categorized based on varied sole aspects. In MANET, it has separated into active and passive attacks. The attack in which the authorized node (attacker) changes or destroys the information and it is communicated in the network is termed as Active attack. Types of active attack such as Black hole Attack, Denial of service (DoS) attack, Worm hole Attack, Grey hole Attacks and so on. The attack in which an unauthorized node obtains the data without disturbing the network operation is named a passive attack. These types of attacks are Traffic Monitoring, Traffic Analysis and

**CONTACT** A. S. Narmadha narmadha.asn@gmail.com Department of ECE, Hindusthan Institute of technology, Coimbatore 641032, India

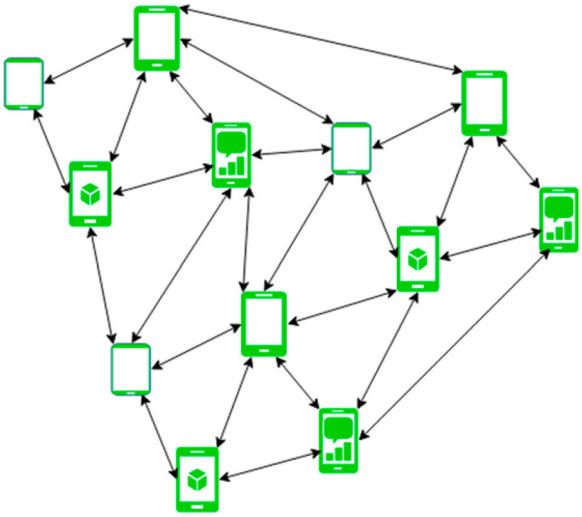

**Figure 1.** Basic MANET architecture.

Eavesdropping. However, MANETs are highly vulnerable to various security attacks due to their inherent characteristics. Hence, to address the issue, AODV is utilized for MANET for discovering the communication route from the source to the destination node. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing with higher attack detection rate, minimum delay and time.

The rest of the paper is organized as follows: A detailed literature review of the previous works is provided in Section 2. Section 3 describes the methods and materials employed in this research including the proposed DNLPPR-WMNDI approach and Section 4 provides simulation metrics and evaluated results. Also, the performance analysis of the proposed technique is presented. The conclusion of this paper is given in Section 5.

## 2. Related works

Over the past few years, numerous works have been carried out in addressing the security issues of MANETs. This section presents a detailed review of the different protocols and techniques modelled over the years.

Authentication in a layered approach was presented [1] with multiple lines of defense for mobile ad hoc networks. The layered security approach was described and design criteria for creating a secure ad hoc network using multiple authentication protocols were analyzed. But, the attack detection rate was not improved. Machine learning algorithms were developed in [2] for computing the local anomaly indexes of MANET routing protocols. However, the attack detection time was not reduced by Machine learning algorithms. But, the packet delivery ratio was not improved. The computation techniques were developed in [3] with genetic programming and grammatical evolution to evolve intrusion detection programmes for challenging environments in MANET. However, the delay was not minimized. An IDS mechanism was designed in [4] to accurately detect and isolate node misbehaviour in the OLSR protocol. But the computational cost was not reduced by the IDS mechanism.

Fuzzy based intrusion detection model was developed in [5] to identify malicious node behaviour. An intelligent detection model called CEAP was proposed in [6] to increase the detection rate and minimal overhead in VANETs. Though overhead was minimized, the computational cost was not minimized.

A detailed review of the optimization approach was presented in [7] for computer security. But the delay was not minimized. The fish algorithm-based protocol was introduced in [8] to allow trustworthy intermediate nodes to participate in path construction protocol without jeopardizing the anonymity of communicating nodes. However, the attack detection rate was not improved by the fish algorithm-based protocol. An On-Demand Trust-Based Multicast Routing protocol (ODTMRP) was developed in [9] for attaining higher security with a packet delivery ratio. But the delay of multicast routing was not minimized.

Work on the end-to-end process designed method reduced the delay [10]. However, a higher security level was not obtained as it failed to perform the attack isolation [11]. The designed framework failed to improve the security of multicast routing in MANET. The designed fuzzy-based routing method in [12] increased the malicious node detection efficiency with minimum delay. Timer-Based Baited Technique (TBBT) was introduced in [13] for black-hole node detection and isolation. The flooding detection-based designed algorithm in [14] improved the data packet delivery ratio. However, it failed in identifying other network attacks in MANET.

A cross-layer-based lightweight, reliable, and secure multicast routing protocol was designed in [15] for improving the attack detection accuracy and packet delivery ratio. But the attack detection time was not minimized. Works were carried out using neural network architectures [16] and multicast routing [17], but it failed to perform the attack detection to further improve the higher packet delivery ratio.

Node Detection and Isolation method [18] improved the packet delivery. A novel flooding factor-based model was introduced in [19] to detect the attacker nodes. But the attack detection rate was not improved. A honey pot-based dynamic anomaly detection method was developed in [20] with cross-layer security. The designed mechanism improved packet delivery and reduced minimum end-to-end delay. However, the attack detection time was not minimized.

Bernoulli Bayesian model was introduced in [21] to monitor and detect malicious node behaviour depending on the classification performance. But the designed model failed to consider the minimum time for attack detection. Avoiding and Isolating Flooding Attacks

using AODV Protocol was designed in [22]. The designed method failed to use any machine learning technique for improving the attack detection rate. A trust-Based Secure Routing Protocol was introduced in [23] based on the fuzzy rule-based approach. The developed technique failed to enhance the security of data communication. A detection and Prevention System (DPS) was developed in [24] to identify and avoid malicious nodes. The designed system minimized the packet drop. However, it failed to reduce the end-to-end delay.

The fuzzy logic technique [25] identified black hole attacks based on trust during route discovery. The designed approach reduced the delay in data transmission. A novel enhanced protocol of AODV was developed in [26] to locate and prevent the black hole nodes. But, it failed to conduct and test the performance of the proposed protocol with various metrics. Anomaly-based Behavioural Detection was performed [27] using a support vector machine. The designed approach improved the accuracy of anomaly detection. However, the time consumption was not minimized. An invincible AODV protocol was developed in [28] to identify the black hole and grey hole nodes. But the detection rate and time performance were not calculated in this work.

A work developed an efficient fuzzy clustering-based algorithm in [29] for intrusion detection of MANET implementation in the cloud storage environment. The works related to multi-cluster Head anomaly were developed in [30]. However, the detection rate was not improved to the expected percentage. An efficient stream region sink position analysis (ESRSPA) model was introduced in [31] for increasing attack detection in mobile ad-hoc networks (MANETs). Attack detection was carried out for identifying the malicious nodes in the system. But the percentage of attack detection was not improved to the maximum possible level. Cross Centric Intrusion Detection System for Secure Routing over Black Hole Attacks in MANETs' was developed in [32].

A two-stage classification technique termed as adaptive Support Vector Machine classification has been proposed with Intrusion Detection System (IDS). An acknowledgment-based method was employed for reporting the malicious sensor nodes. But the limitation was the elapsing higher time [33]. A scheme was proposed in [34] by Adaptive Neuro-Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO) for mobile ad hoc networks to detect the black hole attack and the limitation was that it elapsed more time. Several variants of black hole attack were presented with shortcomings of the present literature. A comprehensive taxonomy of mitigation and detection mechanisms along with summarization related to categories was discussed in [35–37].

### 2.1. Motivation of the research study

Security is a primary constraint in MANETs to preserve communication between mobile nodes. Recently, security issues in MANETs have gained attraction among numerous researchers and hence the concentration on security aspects of MANETs which includes malicious node detection, isolation, securing routing protocols, and response to the malicious node detection has also become primary importance. Due to this, a novel deep learning model is developed in this work to achieve higher security in multicast routing. The deep learning model is ability to learn unsupervised drives continuous improvement in accuracy and outcomes. It also offers data scientists with more reliable and concise analysis results. Consequently, a deep learning model is used in this research.

The issues identified from the existing techniques are a lesser packet delivery ratio, higher delay, higher packet loss, higher computational cost, higher computational complexity, higher attack detection time, and lesser attack detection rate. In order to overcome the observed limitations, the Deep Neural Learned Projective Pursuit Regression-based Watchdog Malicious Node Detection and Isolation (DNLPPR-WMNDI) technique is introduced in MANET. The key objective of the DNLPPR-WMNDI technique is to perform attack detection and isolation for attaining better-improved communication security during the multicast routing in MANETs. The novelty or major contributions involved in the work is described as follows.

- The proposed DNLPPR-WMNDI technique is developed to achieve effective communication security of multicast routing in MANET with a higher packet delivery ratio with less time.
- The projection pursuit regression function is used in the DNLPPR-WMNDI technique to identify the neighbouring nodes between the source and multiple destinations with the help of the time of flight method.
- Watchdog Malicious Node Detection and Isolation (WMNDI) technique is designed to improve the attack detection rate by detecting the malicious node based on the data forwarding time.
- The watchdog timer is used to increase the packet delivery ratio and effectively identify the attacker node and isolate the malicious node. This in turn helps to minimize the end-to-end delay of data transmission in multicast routing in MANET.

## 3. Materials and methods

MANET is vulnerable to security attacks due to the lack of a trusted centralized authority. The attacks disturb, modify or interrupt the routing between the

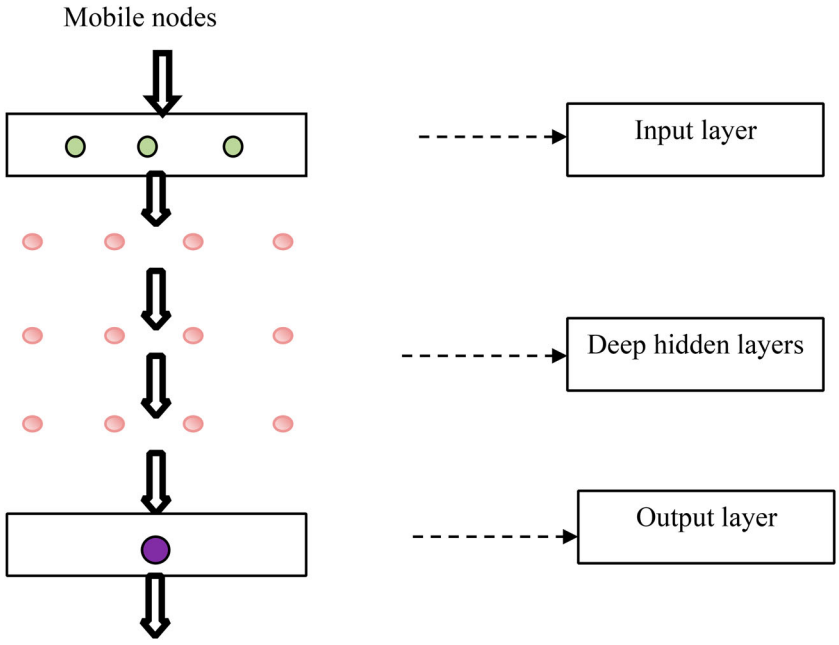


**Figure 2.** Structure of Deep neural learning-based attack detection and isolation.

nodes. Some of the recent works related to secured routing in MANET are reviewed. Based on this motivation, an attack detection and isolation technique called DNLPPR-WMNDI is introduced for improvising the network security during multicast routing in MANETs.

In DNLPPR-WMNDI, MANET is an undirected graph "$G(V, E)$" where "$V$" is the no. of mobile nodes "$mn_1, mn_2, .., mn_n$" distributed in "$N * N$" dimension over the transmission range. In a graph, "$E$" specifies a communication link among the network nodes. In multicasting routing, the source "$SN$"node sends the data packets "$DP_i = DP_1, DP_2, \ldots, DP_n$" to the multiple destination nodes "$DN_1, DN_2, DN_3 \ldots., DN_n$" through the intermediate nodes "$IN_i = IN_1, IN_2, \ldots, IN_n$". Among the multiple intermediate nodes, the malicious nodes are identified based on the Time-of-flight principle and isolated from the network to improve the communication security in MANET.

### 3.1. Novel deep neural network projective pursuit regression model

The new DNLPPR-WMNDI technique is proposed for MANET with the aim of improving communication security. The DNLPPR-WMNDI technique uses the deep neural learning concept for secure multicast routing in MANET by involving four processes namely neighbour node selection, route path discovery, attack detection and isolation. The deep learning technique is incorporated into the back-propagation neural network model and the developed training algorithm forms a machine learning algorithm utilizing several layers to learn the input.

Figure 2 shows the structure of deep neural learning which uses multiple layers to progressively analyze the input. In deep learning, each layer learns the input from the previous layer and transforms it into the next consecutive layers. The architecture is modelled with fully interconnected neurones with interlinked weights on all the connections. As shown in Figure 2, one input layer, three hidden layers and one output layer are used. The activity of the neurones in the input layer "$i(t)$" is expressed as,

$$i(t) = \sum_{i=1}^{n} mn_i * \varphi_1 + c \tag{1}$$

Where the input layer combines the input i.e. mobile nodes "$mn_i$" with weights denoted as "$\varphi_1$" between the input and hidden layer and it is randomly assigned, bias term is denoted as "$c$" and the value is 1, "$i(t)$" indicates the activity of a neurone in the input layer at a time "$t$". The mobile nodes in the input layer are transformed into the first hidden layer. In that layer, the neighbouring nodes are identified from the source to multiple destinations for multicast routing. The steepest descent projection pursuit regression is the machine learning technique used to find the neighbouring nodes. Initially, the source node sends the beacon messages to all the nodes in the network. Figure 3 shows the architecture of the deep learning neural network regression model devised to detect malicious nodes in MANETs.

The training of the new deep neural learning network model in DNLPPR-WMNDI is carried out based on the following methods,

(i) Pre-training of the deep neural learning projective model with un-supervised learning algorithms

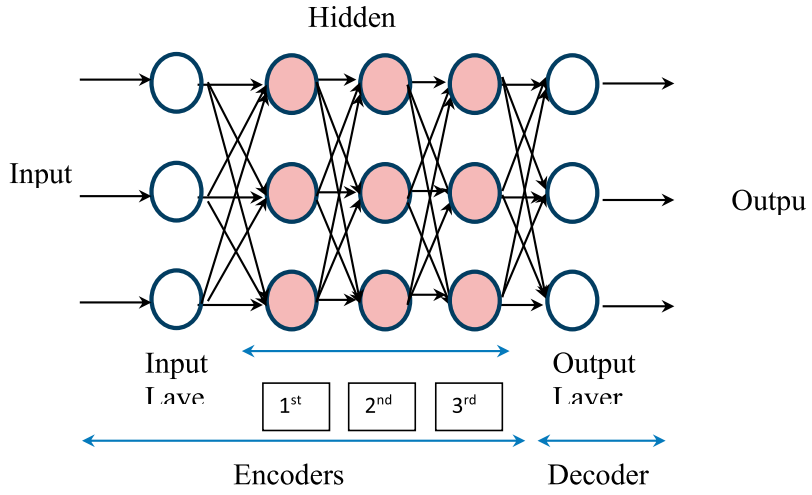


**Figure 3.** Structure of deep learning neural regression model.

(ii) Fine-tuning of the deep neural learning projective model using back propagation neural network gradient descent learning rule.

In the deep learning method, auto encoders are modelled using an unsupervised learning technique. An auto encoder includes two parts as encoder and a decoder. The first half that exchanges the data into the narrow region is named the encoding portion and the second half that alters it back into the original data is termed the decoding portion. This is because the purpose of the auto encoder is to initialize the hidden layer parameters that will reconstruct the high dimensional input data. The encoder transforms the current input data in high dimensional space into codes of low dimensional space. The decoder in the deep neural learning regression model reconstructs the inputs from the respective node neurones. Here, the encoding vector is,

$$Encode\_vector = Enf(Measured\_value) \tag{2}$$

Where, "*Enf*" is the encoding function and decoder carries out the reconstruction mechanism given by "*Def*". The reconstructed output is given by,

$$reconstruct\_vector = Def(Encode\_vector) \tag{3}$$

The key objective of the deep neural learning is to minimize the error observed at reconstruction period. The error is a loss function and is the difference that exists among the encoded and decoded data samples.

$$E_{absolute}(e, \Delta e) = \frac{1}{NI}\sum_{v=1}^{NI} E(Measured\_value, Def(Enf(Measured\_value))) \tag{4}$$

In the new deep neural learning projective pursuit regression (DNLPPR) model, the non-linearity that is present with the encoder and decoder is given by,

$$Enf(x) = Act_{fn}\_encode(W_0 + W_x)$$
$$Def(x) = Act_{fn}\_decode(W_0 + W_x^T) \tag{5}$$

Where, $Act_{fn\_encode}$ and $Act_{fn\_decode}$ denotes activation function of the encoders and decoders, $W_0$ specifies the neural network bias and $W_x$ $W_x^T$ indicate the corresponding weight matrices. To carry out deep learning-based training process, the "*NI*" auto encoders are trained earlier to that of the other neurones stacked. The training of the encoders is given by,

$$Encode\_vector1 = Enf1(Measured\_value) \tag{6}$$

Hence, the input data to the network model is "*Encode_vector1*", the subsequent hidden layers of the DNLPPR are designed with the following auto encoder. Similarly, the above step continues till N-th auto encoder and this is given by,

$$Encode\_vectorN = Enf\_N(Encode\_vector(N-1)) \tag{7}$$

Where, "*Enf_N*" indicates the N-th trained metric of the encoder of DNLPPR. Here, deep hidden layers are pre-trained to overcome local minima and increase the generalization and learning ability. After the completion of pre-training, the fine-tuning process is done. Based on the input *Measured_value*, the output of the DNLPPR model is obtained as,

$$Output\_y = Enf_{N+1}(Encode\_vector\_N) \tag{8}$$

Where, "$Enf_{N+1}$" denote the parameter set that pertains that of the output layer.

The error formulation of the deep learning model is defined by,

$$Mean\_SqError(\mu) = \frac{1}{NI}\sum_{i=1}^{NI} E(Evaluated_{output}, Desired_{target}) \tag{9}$$

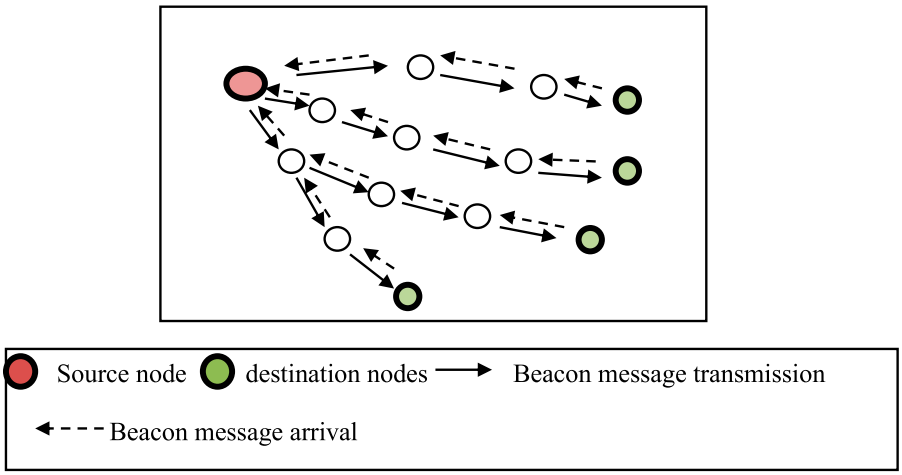


**Figure 4.** Time-of-Flight principle.

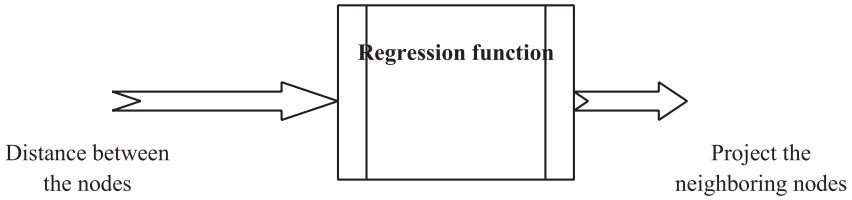


**Figure 5.** Projection pursuit regression function.

Where "$Desired_{target}$" indicate the set target of the given system model. Equations (1)–(9) is utilized to perform the auto encoder process for reconstructing the high dimensional input data.

Figure 4 illustrates the Time-of-Flight principle between the source and destinations. This principle is employed to compute the distance across the mobile nodes based on the beacon message transmission time and its return to the source node. Therefore, the distance between the source and the other node is calculated as follows,

$$d = At_B - Tt_B \tag{10}$$

Where, "$d$" represent the distance between the nodes, $At_B$ indicates a beacon message arrival time and "$Tt_B$" denotes a beacon message transmitting time. In this way, the distance between the sensor nodes is measured by using Equation (10) within the network. Then the regression function analyzes the distances of the mobile nodes.

Figure 5 shows the projection pursuit regression function uses the steepest gradient descent function to find the minimum distance which is mathematically formulated as follows,

$$F(x) = argmind \tag{11}$$

Where "$F(x)$" denotes the steepest gradient-descent rule, *argmin* specifies minimal value, $d$ indicates the distance function. Equation (11) is utilized for determining the minimum distance. Therefore, the regression function projects the minimum distance node as a neighbouring node for data packet transmission. In order to find the route paths, two control messages namely RREQ and RREP are distributed by a source node to multiple destinations through the intermediate nodes. The source mobile node *SN* sends RREQ to multiple destination mobile nodes *DNs* for establishing the multiple route paths by using Equation (12).

$$SNRREQ \rightarrow IN_iRREQ \rightarrow DNs \tag{12}$$

The destination mobile node *DNs* perform as in Equation (13), to *SN* via $IN_i$.

$$SNRREP \leftarrow IN_iRREP \leftarrow DN \tag{13}$$

If the *DNs* sends a reply message to the source *SN*, the path is established and should be used.

At the third hidden layer of the DLNPPR, malicious nodes and normal nodes are correctly identified along the route path using Watchdog Malicious Node Detection and Isolation (WMNDI) technique based on the data packet forwarding time. WMNDI technique detects malicious nodes with the help of the timer. The Node Isolation Attack is a Denial of Service (DOS) attack to isolate the data transmission among the group of mobile nodes. Therefore, the attacker node prevents the data communication of a specific node or group of nodes to the whole network. The Watchdog is used to monitor the activities (i.e. data forwarding time) of mobile nodes. For each node, the forwarding time is

measured as follows,

$$T_f = \sum_{i=1}^{n} tt(DP_i) \tag{14}$$

Where, "$T_f$" denotes a data forwarding time, $tt(DP_i)$ denotes the transmitting time of the data packets. Then the threshold is set to find the malicious or normal node along the route path.

$$Y = \{T_f < \delta; Normal\ node\ otherwise, Malicious\ node \tag{15}$$

From (15), $Y$ denotes an output function, $T_f$ indicates the data forwarding time and $\delta$ specifies a threshold for data forwarding time. If the data forwarding time of a particular mobile node is lesser than the threshold, then the node is said to be a normal node. Otherwise, the node is identified as a malicious node. In Equations (14), and (15), data forwarding time is employed to get a malicious node.

Consider the network scenario of seven mobile nodes; the source node wants to communicate with the destination node. Due to the open environment of the network, there are also malicious nodes available. The attack in which the attacker node coloured in orange has avoided the data packet forwarding and then the attacker nodes prevent link information and stop the data communication to the whole network as shown in Figure 6. For better communication in-network, the attacker node is removed from the network and selects the next hop for the communication from source to destination. This, in turn, helps to improve communication security in MANET. The output of hidden layers at a time "$t$" is obtained as follows,

$$b(t) = \varphi_1 * mn_i + \varphi_2 * b_{(t-1)} \tag{16}$$

From (16), $b(t)$ indicates hidden layer output, $b_{(t-1)}$ specifies output from the previous hidden layer and "$\varphi_2$" indicate hidden layer weights, $\varphi_1$ denotes a weighted interconnection from input to hidden layers, $mn_i$ specifies the input. The results from the hidden layer are forwarded to output layer. At the output layer, the next one-hop neighbouring node is selected for secure transmission from the source to the destination. Based on the deep learning analysis, communication security is improved with minimum delay. The algorithm for obtaining secure communication in MANET is given in Table 1.

Table 1 presents the algorithm developed for deep learning-based malicious node detection and isolation in MANET. The different processes are learned in multiple layers. The input layer receives the mobile nodes and the neighbouring node selection is performed at the first hidden layer using the regression analysis. Based on the regression analysis, the node with minimum distance is projected as neighbours. Then the attack detection and isolation are performed at a third hidden layer with the help of a watchdog timer. The watchdog timer monitors the data forwarding time of each mobile node in the route path. When the node forwards the incoming data packets to the next neighbouring nodes within the threshold, it's a normal node. Else, the mobile node is identified as an attacker node. Finally, the attacker node is removed from the route path and selects the next-hop node for transmitting the data packets toward the destination at higher communication security and minimum delay. As a result, the proposed DNLPPR-WMNDI technique improves multicast routing with a higher security level.

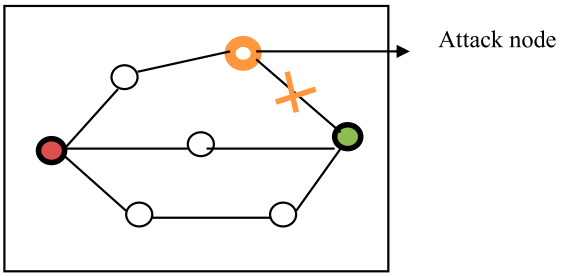


**Figure 6.** Node isolation attack.

**Table 1.** New DNLPPR-WMNDI Algorithm.

**Input:** Number of mobile nodes $mn_1, mn_2, .., mn_n$,
**Output:** Improve data communication security
**Begin**
**1.** Give $mn_i$ to the input layer with the weight $\varphi_1$ **(Input layer)**
**/Neighbouring node selection at first hidden layer**
**2. For each** $mn_i$
**3.** Measure the distance d
**4.** Perform regression analysis
**5.** Find minimum distance $F(x) = \text{argmin } d$
**6.** Identify the neighbouring nodes
**7. end for**
**/Route path selection at the second hidden layer**
**8.** SN sends requests RREQ to DNs via neighbouring nodes
**9.** DNs sends a reply RREPto the SN node
**10.** Construct route paths between SN and DNs
**/Malicious node detection and isolation at the third hidden layer**
**11.** For each $mn_i$ in route path
**12.** Compute data forwarding time $T_f$
**13. If** $(T_f < \delta)$ then
**14.** The node is said to be a normal node
**15. Else**
**16.** The node is said to be a malicious node
**17.** Remove the malicious node from the path
**18. End if**
**/secured communication at the output layer**
**19.** Select next one-hop neighbouring node
**20.** Transmits the data packets to destinations
**End**

## 4. Simulation results and performance analysis

Simulation of the proposed DNLPPR-WMNDI approach and previous methods namely ODTMRP [1], and QASEC [2] are done in the NS2.34 simulator. WSN-DS dataset is utilized for secure data transmission in MANET. The dataset is taken from https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds. This dataset includes 23 features such as Node

**Table 2.** Parametric values.

| Metrics | Value |
|---|---|
| Simulator | NS2 .34 |
| Protocol | AODV |
| No. of mobile nodes | 50,100,150,200,250,300,350,400,450,500 |
| Simulation time | 250 sec |
| Mobility model | Random Way Point model |
| Nodes speed | 0–20 m/s |
| Network area | 1200 m ∗ 1200m |
| Data packets | 15,30,45,60,75,90,105,120,135,150 |
| No. of trial runs | 10 |
| Traffic model | CBR |

**Table 3.** Hyper parameters and description.

| S. No | Hyper parameters | Description |
|---|---|---|
| 1 | Number of hidden layers | Three hidden layers are used |
| 2 | Activation function used in hidden layers | Steepest descent projection pursuit regression, Watchdog Malicious Node Detection, and Isolation is used in the hidden layer |
| 3 | Activation function used in the output layer | Secure communication (i.e. next one-hop neighbouring node is selected) |
| 4 | Learning rate | The value of the learning rate used in our work is 0.001 |
| 7 | Bias | 1 |
| 8 | Weight | Randomly assigned |

**Table 4.** Table for communication layer security threats in the proposed technique.

| Security Threats | Layer Type of proposed technique |
|---|---|
| Black hole Attack, DoS attack, Worm hole Attack, Grey hole Attack | Detection |
| Traffic analysis, difference of network hardware and protocol | Network |
| Secure communication | Application |

ID, Time, Data Sent; Data received, Attack type and so on. The dataset size is 5MB. The data is collected from WSN-DS. Deep neural learning has been trained on the dataset to find different attacks. The various nodes are distributed in a square area of $A^2$ (1200 m ∗ 1200 m). The Random Waypoint model is used as a mobility model to perform multicast routing in MANET. The no. of data packets varied from 15 to 150. Table 2 presents the parametric values employed during the simulation process. The simulation results of the developed DNLPPR-WMNDI approach and that of previous approaches ODTMRP [1], and QASEC [2] are considered for comparison (Table 3).

The communication technologies such as are communication layer, network layer and application layer used in Table 4. The proposed technique using the NS2.34 simulator diagram is given in Figure 7.

In the current healthcare scenario, mobile phones has a crucial part to perform secure text communications between different entities such as doctors, patients, hospitals, ambulances and other healthcare systems. Let's consider the number of mobile nodes in a MANET for transmitting the information i.e. data packets by making secure data communication between mobile nodes. DNLPPR-WMNDI is proposed to discover the attacker node and normal node. Then, an attacker node gets eliminated for secure data communication. The source mobile node forwards the data packets to the control centre during emergency cases. By using the proposed technique, the data is (i.e. source mobile node takes less delay time) to reach the control centre (i.e. destination mobile node) through the help of deep neural learning, projection pursuit regression and watchdog-based attack detection for a route path.

### 4.1. Attack detection rate

The attack detection rate is measured based on the Equation (17) for multicasting routing as given below,

$$ADR = \left( \frac{\begin{array}{c} number\ of\ mobile\ nodes\ correctly \\ detected\ as\ normal\ or \\ malicious\ node \end{array}}{n} \right) * 100 \tag{17}$$

Where "$n$" specifies no. of mobile nodes. Therefore, the ADR is computed with respect to percentages (%). The higher the attack detection rate, the approach is said to be more efficient. The evaluation procedure carried out includes,

- **Existing ODTMRP**: The attack detection rate is estimated as given below,

$$ADR = \left( \frac{44}{50} \right) * 100 = 88\%$$

- **Existing QASEC: T**he attack detection rate is estimated as given below,

$$ADR = \left( \frac{42}{50} \right) * 100 = 84\%$$

- **Proposed DNLPPR-WMNDI: T**he attack detection rate is estimated as given below,

$$ADR = \left( \frac{48}{50} \right) * 100 = 96\%$$

Table 5 presents the solutions and performance of the attack detection rate of three techniques namely DNLPPR-WMNDI and existing methods ODTMRP [1], QASEC [2]. The ten different results of three different techniques show that the attack detection rate is minimized using the DNLPPR-WMNDI approach in comparison with the earlier developed approaches. The results of the attack detection rate are provided in Figure 8.

Computed solutions of attack detection rate using three different techniques namely DNLPPR-WMNDI

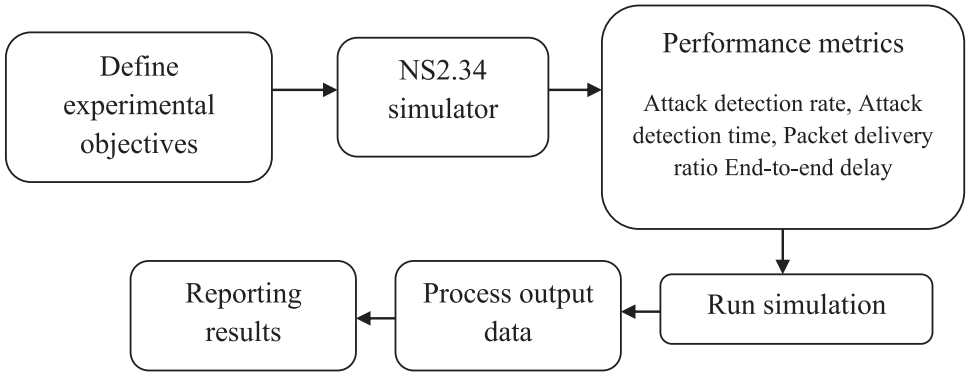


**Figure 7.** NS2.34 simulators using the proposed technique.

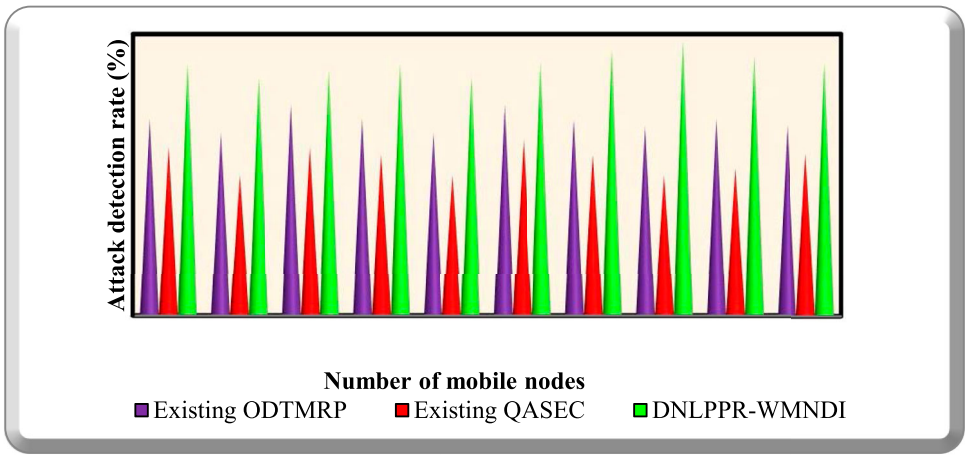


**Figure 8.** Comparison plot of attack detection rate using proposed technique.

**Table 5.** Attack detection rate versus the number of mobile nodes.

| | Attack detection rate (%) | | |
|---|---|---|---|
| Number of mobile nodes | Existing ODTMRP | Existing QASEC | New DNLPPR-WMNDI |
| 50 | 88 | 84 | 96 |
| 100 | 86 | 80 | 94 |
| 150 | 90 | 84 | 95 |
| 200 | 88 | 83 | 96 |
| 250 | 86 | 80 | 94 |
| 300 | 90 | 85 | 96 |
| 350 | 88 | 83 | 98 |
| 400 | 87 | 80 | 99 |
| 450 | 88 | 81 | 97 |
| 500 | 87 | 83 | 96 |

and existing methods ODTMRP [1], and QASEC [2] are shown in Figure 7. In order to find the malicious attack or normal node in multicast routing, the range of mobile nodes is from 50 to 500. The comparison plot shows that the DNLPPR-WMNDI technique improves the attack detection rate more than the existing methods. This is because of applying the deep learning approach which uses the watchdog-based attack detection. Totally ten results of attack detection rate are obtained for each technique. The results of the DNLPPR-WMNDI approach are compared with previous approaches to prove their effectiveness.

### 4.2. Attack detection time

Attack detection time is measured to be the amount of time required to identify the normal or affected node in MANET. Hence, the overall attack detection time is mathematically evaluated as,

$$ADT = n * t(detecting\ one\ node) \tag{18}$$

Where "$n$" specifies the no. of mobile nodes, $t$ indicates a time for identifying the single mobile nodes as normal or malicious. Hence, the ADT is measured in terms of milliseconds (ms). The lesser the attack detection time, the method is said to be more efficient.

- **Existing ODTMRP**: Let us consider the number of is 50 and the time for identifying the single mobile node is $0.4ms$. Hence, the overall attack detection time becomes,

$$ADT = 50 * 0.4ms = 20ms$$

- **Existing QASEC:** Let us consider the numbers of is 50 and the time for identifying the single mobile node is $0.44ms$. Hence, the overall attack detection time is estimated as given below,

$$ADT = 50 * 0.44ms = 22ms$$

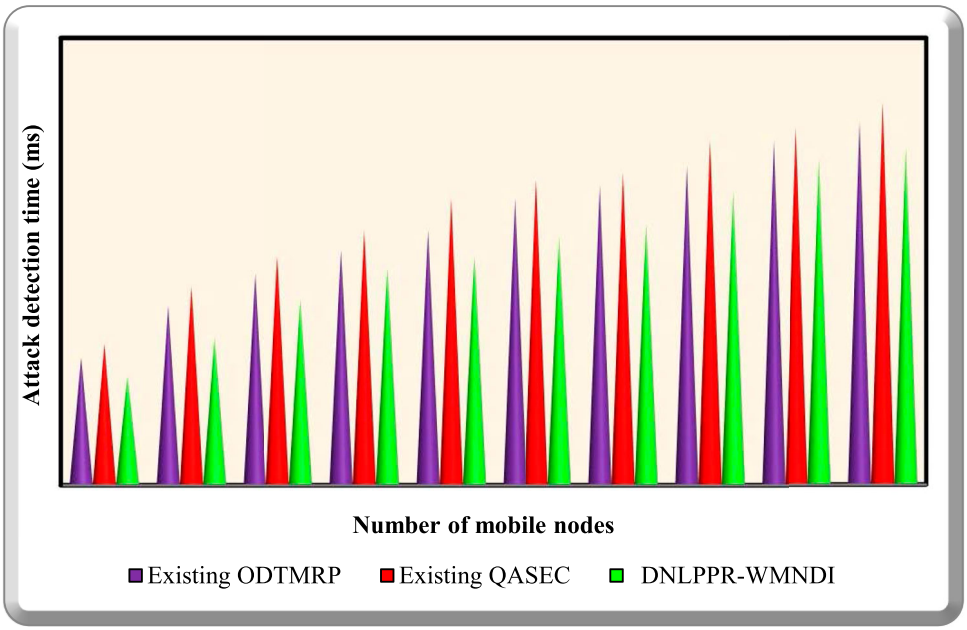


**Figure 9.** Comparison plot of attack detection time using proposed technique.

**Table 6.** Attack detection time versus number of mobile nodes.

| Number of mobile nodes | Attack detection time (ms) | | |
|---|---|---|---|
| | Existing ODTMRP | Existing QASEC | New DNLPPR-WMNDI |
| 50 | 20 | 22 | 17 |
| 100 | 28 | 31 | 23 |
| 150 | 33 | 36 | 29 |
| 200 | 37 | 40 | 34 |
| 250 | 40 | 45 | 36 |
| 300 | 45 | 48 | 39 |
| 350 | 47 | 49 | 41 |
| 400 | 50 | 54 | 46 |
| 450 | 54 | 56 | 51 |
| 500 | 57 | 60 | 53 |

- **Proposed DNLPPR-WMNDI:** Let us consider the numbers of is 50 and the time for identifying the single mobile node is 0.34*ms*. Hence, the overall attack detection time is estimated to be,

$$ADT = 50 * 0.34ms = 17ms$$

Table 6 shows the attack detection time with that of the no. of mobile nodes. While verifying the no. of mobile nodes in the simulation scenario, the various results of attack detection time are obtained. The obtained results show that the DNLPPR-WMNDI technique minimizes the attack detection time. The comparative plot based on the simulation results of three different techniques is shown in Figure 8.

Figure 9 illustrates the graphical representation of attack detection time. The watchdog timer-based attack detection only considers the data forwarding time from one to another node. Then the forwarding time is evaluated by setting the threshold value. The node which has lesser data forwarding time than the threshold is said to a normal. The node which delays the data packet to be forwarded is said to be an attacker node. Let us consider 50 mobile nodes in the simulation scenario. The DNLPPR-WMNDI technique took 17*ms* of attack detection time whereas the 20*ms* and 22*ms* time taken by the ODTMRP [1], QASEC [2]. Similarly, the various inputs are taken, and calculating the attack detection time. The average of comparison results proves the attack detection time is minimized by 11% using the DNLPPR-WMNDI technique in comparison with the previous approach ODTMRP [1] and 17% compared to QASEC [2].

### 4.3. Packet delivery ratio

The packet delivery ratio is the number of data packets correctly received from the number of data packets sent. The formula for calculating the data security level is given below,

$$DPDR = \left(\frac{Number\ of\ DP\ correctly\ received}{Number\ of\ DP\ sent}\right) * 100 \tag{19}$$

Where "*DPDR*" denotes the data packet delivery ratio, "*DP*" represents the no. of data packets perfectly received at the destination. The *DPDR* is evaluated by percentage (%).

- Existing ODTMRP: The DPDR is mathematically calculated to be,

$$DPDR = \left(\frac{13}{15}\right) * 100 = 86.66\% \sim 87\%$$

- Existing QASEC: The DPDR is mathematically calculated by,

$$DPDR = \left(\frac{12}{15}\right) * 100 = 80\%$$

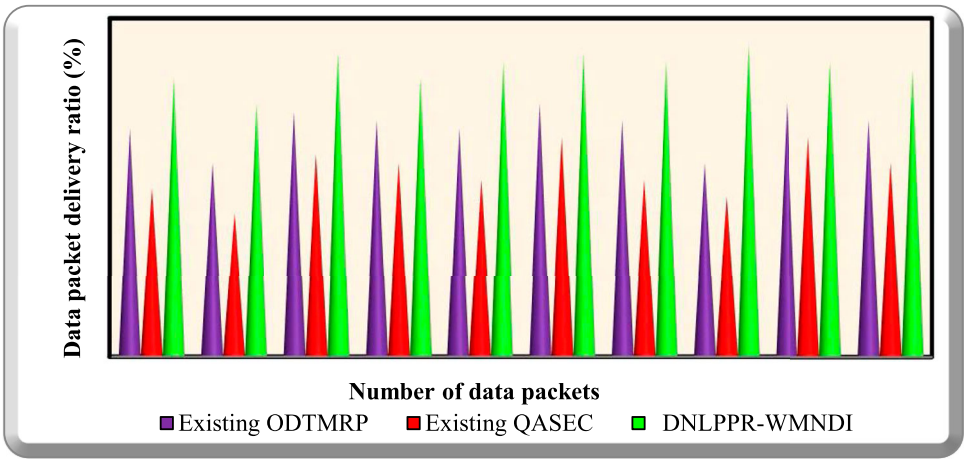


**Figure 10.** Comparison plot of packet delivery ratio using proposed technique.

**Table 7.** Data packet delivery ratio versus the number of data.

| | Data packet delivery ratio (%) | | |
|---|---|---|---|
| Number of data packets | Existing ODTMRP | Existing QASEC | DNLPPR-WMNDI |
| 15 | 87 | 80 | 93 |
| 30 | 83 | 77 | 90 |
| 45 | 89 | 84 | 96 |
| 60 | 88 | 83 | 93 |
| 75 | 87 | 81 | 95 |
| 90 | 90 | 86 | 96 |
| 105 | 88 | 81 | 95 |
| 120 | 83 | 79 | 97 |
| 135 | 90 | 86 | 95 |
| 150 | 88 | 83 | 94 |

- Proposed DNLPPR-WMNDI: Let us consider the no. of data packets correctly received as 14, and the total no. of data packets sent as 15. Therefore, the data security level is mathematically calculated by,

$$DPDR = \left(\frac{14}{15}\right) * 100 = 93.33\%$$

Table 7 clearly shows the comparative solutions and in multicast routing, the source node sends the data packets to multiple destinations. The comparison plot of the data packet delivery ratio with that of the no. of data packets is shown in Figure 9 and it confirms that the considered metric is improved using the DNLPPR-WMNDI technique. This is because of DNLPPR-WMNDI technique initially selects the neighbouring nodes based on the distance measure. Then the route paths between the source and multiple destinations are established for secure data transmission. Then the watchdog timer effectively identifies the attacker node. Then the attacker node is isolated from the current path and selects the next-hop node to forward the data packets. Due to this, the data packets get perfectly distributed at the destination. As a result, the security level of data communication gets improved. This is substantiated in the evaluation done (Figure 10).

Consider 15 data packets sent from the source node, 14 data packets are received at the destination and the packet delivery ratio is 93% using the DNLPPR-WMNDI technique. The packet delivery ratio of ODTMRP [1] and QASEC [2] are 87% and 80% respectively. The average of ten results proves that the packet delivery ratio gets increased by 8% and 15% in comparison with ODTMRP [1] and QASEC [2] respectively.

### 4.4. End-to-end delay

End-to-end delay specifies the time difference between the data packet arrival time at the destination and the data packet sending time [38]. The evaluation is done with,

$$EED = Number\ of\ DPs * (DP_{At} - DP_{st}) \quad (20)$$

Where $EED$ indicates end to end delay in milliseconds, $DPs$ denotes data packets, $DP_{At}$ is a data packet arrival time and $DP_{st}$ indicates a data packet sending time.

- **Existing ODTMRP:** Let us consider the no. of data packets to be 15 and the data packet arrival time to be $0.87ms$ and the sending time to be $0ms$. Therefore, the complete end-to-end delay is calculated as follows,

$$EED = 15 * (0.87ms - 0ms) = 13ms$$

- **Existing QASEC**: With the no. of data packets to be 15 and the data packet arrival time is $1ms$ and the sending time is $0ms$. Therefore, the overall end-to-end delay is evaluated to be,

$$EED = 15 * (1ms - 0ms) = 15ms$$

- **Proposed DNLPPR-WMNDI:** The complete end-to-end delay is calculated as follows,

$$EED = 15 * (0.74ms - 0ms) = 11ms$$

Table 8 results prove that the end-to-end delay of DNLPPR-WMNDI is found to be reduced in a significant way than the other two methods. Figure 11 depicts

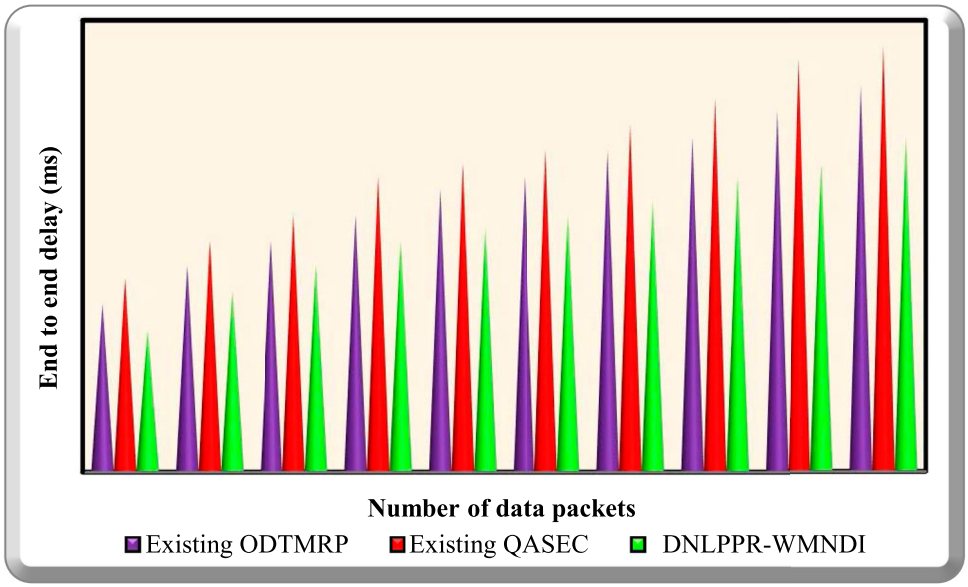


**Figure 11.** Comparison plot for end-to-end delay using proposed technique.

**Table 8.** Delay metric.

| | End to end delay (ms) | | |
|---|---|---|---|
| Number of data packets | Existing ODTMRP | Existing QASEC | DNLPPR-WMNDI |
| 15 | 13 | 15 | 11 |
| 30 | 16 | 18 | 14 |
| 45 | 18 | 20 | 16 |
| 60 | 20 | 23 | 18 |
| 75 | 22 | 24 | 19 |
| 90 | 23 | 25 | 20 |
| 105 | 25 | 27 | 21 |
| 120 | 26 | 29 | 23 |
| 135 | 28 | 32 | 24 |
| 150 | 30 | 33 | 26 |

the graphical representation of the solutions attained. The figure shows the end-to-end delay of DNLPPR-WMNDI is minimized. This significant improvement of the DNLPPR-WMNDI technique is achieved by applying the deep learning technique.

The deep learning technique effectively performs attack detection and isolation to improve data communication with minimum delay. The attacker node in the route path is identified and removed from the route. This, in turn, reduces end-to-end delay. The above discussion shows that the end-to-end delay of the proposed DNLPPR-WMNDI technique is considerably reduced by 13% and 22% than the existing ODTMRP [1] and QASEC [2] respectively. The presented solutions prove lucidly that the proposed DNLPPR-WMNDI approach improves secure data communication in multicast routing with a higher delivery ratio and minimum time.

## 5. Conclusion

An efficient machine learning technique called DNLPPR-WMNDI is introduced for increasing communication security in MANET. During the regression function, the neighbouring nodes from source to destination are identified to construct and find the route path for multicast routing based on the Time of Flight method. Followed by, watchdog timer concept is utilized in deep neural learning to discover the attacker node and normal node in the network. Next, the watchdog timer efficiently finds the attacker node hence, a higher attack detection rate. When there is any attacker in the route path, the other one-hop neighbour is chosen. Subsequently, an attacker node gets removed. The communication security and data packet delivery ratio was enhanced in MANET. In addition, end-to-end delay and time were minimized. Experimental results of the DNLPPR-WMNDI technique significantly improve attack detection rate by 13%, packet delivery ratio by 12%, and minimizes the attack detection time by 14% and end-to-end delay by 18% than the state-of-art methods. In the future, the proposed technique is further extended to execute the effective routing of data packets for large-scale network deployments for superior link quality among mobile nodes in MANET. The better link between nodes leads to improve throughput and lifetime of the network.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Research involving human participants and/or animals

The authors confirm that there was no human participants and/or animals used for this research study.

## Informed consent

No human or animal participation has been involved in conducting this study.

## Data

My manuscript has no associated data.

## References


[1] Komninos N, Vergados DD, Douligeris C. Authentication in a layered security approach for mobile ad hoc networks. Comput Secur. 2007;26(5):373–380. doi:10.1016/j.cose.2006.12.011

[2] Cabrera JB, Gutiérrez C, Mehra RK. Ensemble methods for anomaly detection and distributed intrusion detection in mobile ad-hoc networks. Inf Fusion. 2008;9(1):96–119. doi:10.1016/j.inffus.2007.03.001

[3] Sen S, Clark JA. Evolutionary computation techniques for intrusion detection in mobile ad hoc networks. Comput Netw. 2011;55(15):3441–3457. doi:10.1016/j.comnet.2011.07.001

[4] Abdalla AM, Saroit IA, Kotb A, et al. Misbehavior nodes detection and isolation for MANETs OLSR protocol. Procedia Comput Sci. 2011;3:115–121. doi:10.1016/j.procs.2010.12.020

[5] Balan EV, Priyan MK, Gokulnath C, et al. Fuzzy based intrusion detection systems in MANET. Procedia Comput Sci. 2015;50:109–114. doi:10.1016/j.procs.2015.04.071

[6] Wahab OA, Mourad A, Otrok H, et al. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. Expert Syst Appl. 2016;50:40–54. doi:10.1016/j.eswa.2015.12.006

[7] Fernandes DA, Freire MM, Fazendeiro PA, et al. Applications of artificial immune systems to computer security: A survey. J Inf Secur Appl. 2017;35:138–159. doi:10.1016/j.jisa.2017.06.007

[8] Sathiamoorthy J, Ramakrishnan B. Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs. J Inf Secur Appl. 2017;36:43–58. doi:10.1016/j.jisa.2017.08.001

[9] Xia H, Li Z, Zheng Y, et al. A novel light-weight subjective trust inference framework in MANETs. IEEE Trans Sustain Comput. 2018;5(2):1–13.

[10] Usman M, Jan MA, He X, et al. QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Gener Comput. 2018;109(1):1–21. doi:10.1016/j.future.2018.05.007

[11] Yanga B, Zhenqiang Wu Y, Jiang X. Packet delivery ratio and energy consumption in multicast delay-tolerant MANETs with power control. Comput Netw. 2019;161:150–161. doi:10.1016/j.comnet.2019.06.003

[12] Brindha V, Karthikeyan T, Manimegalai P. Fuzzy enhanced secure multicast routing for improving authentication in MANET. Cluster Comput. 2018;22(6):1–9. doi:10.1007/s10586-017-1282-9

[13] Yasin A, Zant MA. Detecting and isolating black-hole attacks in MANET using timer based baited technique. Wireless Commun Mobile Comput. September 2018;2018:1–10. doi:10.1155/2018/9812135

[14] Luong NT, Vo TT, Hoang D. FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile Ad Hoc networks. Wireless Commun Mobile Comput. January 2019;2019:1–17. doi:10.1155/2019/6869307

[15] Sekar S, Latha B. Lightweight reliable and secure multicasting routing protocol based on cross-layer for MANET. Concurr Comput Practice Exp. 2018;32(4):1–12.

[16] Sowah RA, Ofori-Amanfo KB, Mills GA, et al. Detection and prevention of Man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks (ANN). J Comput Netw Commun. January 2019;2019:1–14. doi:10.1155/2019/4683982

[17] Singal G, Laxmi V, Gaur MS, et al. Multi-constraints link stable multicast routing protocol in MANETs. Ad Hoc Netw. August 2017;63:115–128. doi:10.1016/j.adhoc.2017.05.007

[18] Kavitha T, Geetha K, Muthaiah R. India: intruder node detection and isolation action in mobile Ad Hoc networks using feature optimization and classification approach. J Med Syst. 2019;43:1–7. doi:10.1007/s10916-018-1115-2

[19] Ahmed MN, Abdullah AH, Chizari H, et al. F3TM: flooding factor based trust management framework for secure data transmission in MANETs. J King Saud Univ Comput Inf Sci. July 2017;29(3):269–280. doi:10.1016/j.jksuci.2016.03.004

[20] Usha G, Rajesh Babu M, Saravana Kumar S. Dynamic anomaly detection using cross layer security in MANET. Comput Electr Eng. 2017;59:231–241. doi:10.1016/j.compeleceng.2016.12.002

[21] Rmayti M, Khatoun R, Begriche Y, et al. A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks. Comput Netw. 2017;121:53–64. doi:10.1016/j.comnet.2017.04.027

[22] Zant MA, Yasin A. Avoiding and isolating flooding attack by enhancing AODV MANET protocol (AIF-AODV). Secur Commun Netw. March 2019;2019:1–12. doi:10.1155/2019/8249108

[23] Garga MK, Singh N, Verma P. Fuzzy rule-based approach for design and analysis of a trust-based secure routing protocol for MANETs. Procedia Comput Sci. 2018;132:653–658. doi:10.1016/j.procs.2018.05.064

[24] Khan FA, Imran M, Abbas H, et al. A detection and prevention system against collaborative attacks in mobile Ad hoc networks. Future Gener Comput Syst. 2017;68:416–427. doi:10.1016/j.future.2016.07.010

[25] Arulkumaran G, Gnanamurthy RK. Fuzzy trust approach for detecting black hole attack in mobile adhoc network. Mobile Netw Appl. 2019;24:386–393. doi:10.1007/s11036-017-0912-z

[26] Yaseen QM, Aldwairi M. An enhanced AODV protocol for avoiding black holes in MANET. Procedia Comput Sci. 2018;134:371–376. doi:10.1016/j.procs.2018.07.196

[27] Meddeb R, Jemili F, Triki B, et al. Anomaly-based behavioral detection in mobile Ad-Hoc networks. Procedia Comput Sci. 2019;159:77–86. doi:10.1016/j.procs.2019.09.162

[28] Venu VS, Avula D. Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks. Int J Commun Syst. 2018;31(6):1–19. doi:10.1002/dac.3518

[29] Chen M, Wang N, Zhou H, et al. FCM technique for efficient intrusion detection system for wireless networks in cloud environment. Comput Electr Eng. 2018;71:978–987. doi:10.1016/j.compeleceng.2017.10.011

[30] Sharma S, Kaul A. Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. Veh Commun. 2018;12:23–38. doi:10.1016/j.vehcom.2017.12.003

[31] Vigenesh M, Santhosh R. An efficient stream region sink position analysis model for routing attack detection in mobile ad hoc networks. Comput Electr Eng. 2019;74:273–280. doi:10.1016/j.compeleceng.2019.02.005

[32] Rajendran N, Jawahar PK, Priyadarshini R. Cross centric intrusion detection system for secure routing over

black hole attacks in MANETs. Comput Commun. 2019;148:129–135. doi:10.1016/j.comcom.2019.09.005
[33] Borkar GM, Patil LH, Dalgade D, et al. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustain Comput Inf Syst. 2019;23:120–135. doi:10.1016/j.suscom.2019.06.002
[34] Moudni H, Er-rouidi M, Mouncif H, et al. Black hole attack detection using fuzzy based intrusion detection systems in MANET. Procedia Comput Sci. 2019;151:1176–1181. doi:10.1016/j.procs.2019.04.168
[35] Khanna N, Sachdeva M. A comprehensive taxonomy of schemes to detect and mitigate black hole attack and its variants in MANETs. Comput Sci Rev. 2019;32:24–44. doi:10.1016/j.cosrev.2019.03.001
[36] Masdari M, Khezri H. A survey and taxonomy of the fuzzy signature-based intrusion detection systems. Appl Soft Comput. 2020;92(1):106301. doi:10.1016/j.asoc.2020.106301
[37] Fatemidokht H, Rafsanjani MK. QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. J Syst Softw. 2020;165(1):110561. doi:10.1016/j.jss.2020.110561
[38] Govindaraj S, Deepa SN. Network energy optimization of IOTs in wireless sensor networks using capsule neural network learning model. Wirel Pers Commun. 2020 Dec;115(3):2415–2436. doi:10.1007/s11277-020-07688-2