Delta Ruled First Order Iterative Deep Neural Learning for Sybil and Wormhole Attacks Detection in Healthcare Wireless Sensor Network

John Clement Sunder A (✉ sunderajcece@gmail.com)

Bannari Amman Institute of Technology

Dr. K.P. Sampoomam KP

Bannari Amman Institute of Technology

Dr.R.Vinodkumar R

Sona College of Technology

Research Article

Keywords: Delta Ruled First Order Iterative Deep Learning, Healthcare WSN, Isolation, Sybil Attack, Wormhole Attack

Posted Date: June 3rd, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-512769/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

DELTA RULED FIRST ORDER ITERATIVE DEEP NEURAL LEARNING FOR SYBIL AND WORMHOLE ATTACKS DETECTION IN HEALTHCARE WIRELESS SENSOR NETWORK

Dr. A.John Clement Sunder*, Dr. K.P. Sampooram¹, Dr.R.Vinodkumar²
Assistant Professor*, Professor^{1,2}

Department of Electronics and Communication Engineering*,^{1,2}

Bannari Amman institute of Technology*,¹, Sona College of Technology²

E-mail: sundarajcece@gmail.com*, drsampoornamkp@gmail.com¹, drvinodkumarece@gmail.com²

ABSTRACT

Detection and isolation of Sybil and wormhole attack nodes in healthcare WSN is a significant problem to be resolved. Few research works have been designed to identify Sybil and wormhole attack nodes in the network. However, the detection performance of Sybil and wormhole attack nodes was not effectual as the false alarm rate was higher. In order to overcome such limitations, Delta Ruled First Order Iterative Deep Learning based Intrusion Detection (DRFOIDL-ID) Technique is proposed. The DRFOIDL-ID Technique includes two main phase namely attack detection and isolation. The DRFOIDL-ID Technique constructs Delta Ruled First Order Iterative Deep Learning in attack detection phase with aim of detecting the occurrence of Sybil and wormhole attacks in healthcare WSN. After detecting the attack nodes, DRFOIDL-ID Technique carried out isolation process with the objective of increasing the routing performance. During the isolation phase, DRFOIDL-ID Technique keep always the identified Sybil and wormhole attack nodes through transmitting the isolation messages to all sensor nodes in healthcare WSN. Hence, DRFOIDL-ID Technique improves the routing performance with lower packet loss rate. The DRFOIDL-ID Technique conducts the simulation process using factors such as attack detection rate, attack detection time, false alarm rate and packet loss rate with respect to a diverse number of sensor nodes and data packets. The simulation result proves that the DRFOIDL-ID Technique is able to improve the attack detection rate and also reduces the attack detection time as compared to state-of-the-art works.

Keywords: Delta Ruled First Order Iterative Deep Learning, Healthcare WSN, Isolation, Sybil Attack, Wormhole Attack

1. INTRODUCTION

Sensor nodes in healthcare WSN are exposed to diverse attacks. Thus, Sybil and wormhole attacks are considerable issues to be addressed in a wireless network to attain higher security. A Sybil attack is an attack in which a single adversary manipulates multiple nodes in healthcare WSN. Besides, Wormhole attack is one of the harsh attacks in a wireless sensor network. In existing scenario, many techniques have been developed to recognize Sybil and wormhole attack nodes in the network. But, the detection performance of Sybil and wormhole attack nodes was not sufficient. In order to provide a better solution for detecting the Sybil and wormhole attacks in healthcare WSN, DRFOIDL-ID Technique is designed. An energy trust system (ETS) was intended in [1] to efficiently identify Sybil attacks using identity and position verification. But, the wormhole attack remained unsolved which impacts the attack detection rate. A wormhole detection mechanism was intended in [2] with help of RPL(Routing Protocol for Low Power and Lossy Networks) routing protocol. However, the time required for finding the wormhole detection was more.

Robust and secure time-synchronization protocol (RTSP) was presented in [3] for anomaly detection and to secure network from Sybil attacks. However, the false alarm rate of anomaly detection was not addressed. Deep-regression model was designed in [4] for identification of Sybil attack in the social network. But, the time complexity of Sybil attack detection was very higher. Ad hoc on demand Multipath Distance Vector routing protocol was introduced in [5] for discovery and avoidance of wormhole attack in WSN. However, the attack detection rate was lower. A lightweight sybilfree (SF)-APIT algorithm was developed in [6] for identifying Sybil attacks in distributed wireless localization schemes. However, computational time was more.

A lightweight countermeasure for the wormhole attack called LiteWorp was designed in [7] for detection and isolation of the wormhole attack in static multi-hop wireless networks. However, Sybil attack detection was an open issue. An efficient and lightweight solution was presented in [8] for Sybil attack detection according to the time difference of arrival (TDOA) between the source node and beacon nodes. But, the packet loss rate was higher.

A review of various techniques designed for discovery and mitigation of Sybil attack in the network was analyzed in [9]. A low complexity Sybil attack discovery scheme was intended in [10] with help of signed response (SRES) authentication mechanism. The intrusion detection performance was poor.

In order to resolve the existing issues in intrusion detection, DRFOIDL-ID Technique is introduced. The main contribution of DRFOIDL-ID Technique is shown in below.

- ❖ To achieve improved intrusion detection performance to find the Sybil and wormhole attack nodes in healthcare WSN as compared to state-of-the-art works, DRFOIDL-ID Technique is designed. The DRFOIDL-ID Technique is proposed with the support of delta rule and mean square weighted deviation (MSWD) and first-order iterative optimization algorithm.
- ❖ To enhance the intrusion detection rate as compared to state-of-the-art works, mean square weighted deviation (MSWD) is applied in DRFOIDL-ID Technique. The MSWD measures the difference between the target and actual output to enhance the detection performance of Sybil and wormhole attacks detection in healthcare WSN.
- ❖ To minimize the time taken for detecting the Sybil and wormhole attack nodes in healthcare WSN as compared to state-of-the-art works, delta rule, and a first-order iterative optimization algorithm is used in DRFOIDL-ID Technique.

The rest of this paper is planned as follows. Section 2 demonstrates the related works. Section 3 explains the proposed DRFOIDL-ID Technique with the aid of the architecture diagram. Section 4 and Section 5 shows the experimental settings and performance analysis using parameters. Finally, Section 6 depicts the conclusion of this paper.

2. RELATED WORKS

A Hybrid Fuzzy K-means algorithm was employed in [11] for the detection of Sybil attacks in WSN. A novel technique was designed in [12] by using match-position verification method with message authentication for finding, removing, the Sybil attack nodes in the network. A survey of diverse techniques developed for identification and prevention of Sybil attack in WSN was presented in [13]. The lightweight watchdog-based algorithm was employed in [14] for detecting Sybil intrusions in mobile WSNs.

Fuzzy based Sybil attack detection was introduced in [15] with the application of trapezoidal membership function to minimize the false positive rate. However, packet dropping rate was more. A pairwise key pre-distribution scheme was designed in [16] for wormhole attacks recognition in geographic routing protocols. But, preventing the Sybil attack from WSN remained an open issue. An ultra-wideband (UWB) ranging-based detection algorithm was used in [17] for obtaining higher Sybil attacks detection accuracy and lower false alarm rate in the wireless network. Trust-Based Sybil Detection (TBSD) technique was intended in [18] using manipulative trust values of neighboring sensor nodes.

Impact of Sybil and Wormhole Attacks in WSN was analyzed in [19] with assists of Location Based Geographic Multicast Routing Protocol. A channel-based authentication technique was designed in [20] to detect Sybil attacks in wireless networks, utilizing the uniqueness of channel responses in the rich-scattering environment.

3. DELTA RULED FIRST ORDER ITERATIVE DEEP LEARNING BASED INTRUSION DETECTION TECHNIQUE

The Delta Ruled First Order Iterative Deep Learning based Intrusion Detection (DRFOIDL-ID) Technique is designed to increase the routing performance of healthcare WSN via Sybil and wormhole attack identification and isolation. The DRFOIDL-ID Technique is introduced with applications of delta rule and mean square weighted deviation (MSWD) and first-order iterative optimization algorithm on the contrary to state-of-the-art works. The Delta rule employs an error function to carry out gradient descent learning. Thus, delta rule uses the derivative of the network's weights with respect to the output error to adjust the weights and thereby provides better intrusion detection results as compared to existing work. On the contrary to conventional works, MSWD is employed in DRFOIDL-ID Technique to accurately determine error function during the intrusion detection process. Besides, the first order iterative optimization algorithm is applied in DRFOIDL-ID Technique finds the optimal weights that

reduce error function to accurately detect the Sybil and wormhole attack nodes in healthcare WSN with minimal time. Therefore, DRFOIDL-ID Technique improves the Sybil and wormhole attack detection performance in healthcare WSN.

3.1 System Model

Let consider a healthcare WSN characterized as graph structure ' $G(V_i, E_i)$ ' where ' V_i ' denotes the number of sensor nodes and ' E_i ' indicates links between sensor nodes. The sensor nodes in healthcare WSN i.e. ' $S_i = S_1, S_2, S_3 \dots S_n \in V$ ' are lies within the transmission range ' R '. Nodes in network commune directly with each other using wireless transceivers. Sensor nodes are deployed to observe physical or environmental characteristics such as temperature, sound, vibration, pressure, motion. There are many types of attacks possible in healthcare WSN such as selective forwarding, spoofed or replayed routing information, Sybil attack, sinkhole attack, Hello flood attack , Wormhole attack, etc.

Wormhole attack is one of the significant attacks to be solved as it threatens the network availability via dropping data and disturbing routing paths. In a wormhole attack, a wormhole tunnel is formulated by two malicious nodes where it drops packets from their neighbor nodes. Figure 1 depicts the example of wormhole attack in WSN.

Figure 1: Example of Wormhole Attack in Healthcare WSN

Figure 1 shows an example of a wormhole attack in which the two malicious nodes ' S_1 ' and ' S_2 ' construct a wormhole tunnel through which it redirects the transmissions. The wormhole attack nodes in healthcare WSN change the original routing paths and drop the data going through the wormhole tunnel. Also, the two wormhole attack nodes in network utilize more amount of energy than others. When the energy is exhausted, the sensor network might not work properly. Therefore, wormhole attack nodes compromise the network availability and data privacy and may cause a serious security problem in sensor networks. Thus, detection and isolation of wormhole attack nodes in healthcare WSN is a key problem to be addressed.

Another harmful attack to be resolved in healthcare WSN is a Sybil attack as where same node acts as the different one at the same time. Hence, Sybil attacks impact data integrity, security, and resource utilization. The following Figure 2 shows the example of Sybil attack in WSN.

Figure 2 an Example of Sybil Attack in Healthcare WSN

Figure 2 depicts an example of a Sybil attack where the intrusion node ' S_5 ' communicates with neighboring nodes by using the identity of normal sensor nodes i.e. ' S_6 ' and ' S_7 '. In the Sybil attack, a single node gives many identities in the area to other nodes in healthcare WSN which is an illegal process. In addition, Sybil attack causes confusion in the network and it gets collapsed which impacts the routing performance of healthcare WSN. Thus, discovery and isolation of Sybil attack nodes in healthcare WSN is an essential problem to be addressed. To enhance the detection performance of Sybil and wormhole attacks in healthcare WSN with minimal time consumption, DRFOIDL-ID Technique is proposed. The architecture diagram of DRFOIDL-ID Technique is shown in below.

Figure 3 Architecture Diagram of DRFOIDL-ID Technique for Sybil and Wormhole Attack Detection and Isolation

Figure 3 depicts the overall processes of DRFOIDL-ID Technique to improve routing performance of healthcare WSN through a Sybil and wormhole attacks identification and isolation. As demonstrated in the above figure, DRFOIDL-ID Technique contains two main processes such as attack detection phase and isolation phase. During attack detection phase, DRFOIDL-ID Technique applied Delta Ruled First Order Iterative Deep Learning to effectively identify the Sybil and wormhole attacks in healthcare WSN with higher accuracy rate and lower time.

After finding the intruder nodes, DRFOIDL-ID Technique performs isolation process. During the isolation phase, DRFOIDL-ID Technique separates both, the Sybil and wormhole attack nodes in WSN by broadcasting the isolation messages to all nodes. Thus, DRFOIDL-ID Technique significantly enhances the routing performance of healthcare WSN. The detailed process of DRFOIDL-ID Technique is shown in below.

3.2 Attacks Detection Phase

The attack detection is an initial process in DRFOIDL-ID Technique where it uses Delta Ruled First Order Iterative Deep Learning to find out the occurrences of Sybil and wormhole attack nodes in healthcare WSN. The Delta Ruled First Order Iterative Deep Learning is developed by combining delta rule and mean square weighted deviation (MSWD) and first-order iterative optimization algorithm in the deep learning process. On the contrary to existing intrusion detection techniques, deep learning is employed in DRFOIDL-ID Technique as it serves as a powerful computational tool for resolving prediction, decision, diagnosis, and detection decision problems based on a well-defined computational architecture. Besides that, Deep Learning is the fastest growing field in machine learning. In addition, Delta Ruled First Order Iterative Deep Learning is suitable to train a large size of healthcare WSN (i.e. more number of sensor nodes) through neural network architectures that learn features directly from the sensor nodes without the need for manual feature extraction. This supports for DRFOIDL-ID Technique to precisely detect the Sybil and wormhole attack nodes in large healthcare WSN with minimal time utilization. The process of Delta Ruled First Order Iterative Deep Learning is presented in below.

Figure 4 Process of Delta Ruled First Order Iterative Deep Learning for Intrusion Detection

Figure 4 presents the flow process of Delta Ruled First Order Iterative Deep Learning to perform intrusion detection. As depicted in the above figure, the input layer receives a number of sensor nodes as input. Then, the input layer passes the inputs to the hidden layer. The Delta Ruled First Order Iterative Deep Learning employs number of hidden layers to deeply examine the sensor node behavior in healthcare WSN. Finally, the output layer returns the detection result of the sensor node.

Let us consider a Delta Ruled First Order Iterative Deep Learning takes sensor node ' S_i ' as input. The input layer ' r ' combine the sensor nodes ' S_i ' together with weights and bias term. From that, neurons activity in the input layer ' (p) ' is mathematically formulated as below,

$$p(t) = \sum_{i=1}^n S_i w_{pq} + x_j \quad (1)$$

From (1), the input layer ' r ' unite the input sensor nodes ' S_i ' with weights ' w_{pq} ' and bias term ' x_j ' whereas ' $p(t)$ ' point outs the activity of a neurons in input layer at a time ' t '. Here ' w_{pq} ' indicates a weights between the input ' p ' and hidden layer ' q '. The input layer forwards the input sensor nodes ' S_i ' to the hidden layer. The Delta Ruled First Order Iterative Deep Learning ulitlizes more hidden layers to deeply analyze the behaviour of sensor nodes in healthcare WSN. Thus, neurons activity in hidden layers ' $q_i(t)$ ' is mathematically estimated as below,

$$q_i(t) = A(F) \sum_{i=1}^n p(t) w_q \quad (2)$$

From (2), ' $A(F)$ ' is an activation function and ' $p(t)$ ' is the neurons activity of the input layer whereas ' w_q ' is a weight in hidden layers. here, ' $q_i(t)$ ' represents a neurons activity in hidden layers at a time ' t '. In DRFOIDL-ID Technique, Delta Ruled First Order Iterative Deep Learning used tanh activation function for analyzing the behaviour of senor node. The tanh activation function compares the sensor node behaviour ' $b(S_i)$ ' with Sybil attack node behaviour ' $b(SA)$ ' and wormhole attack node behaviour ' $b(WA)$ ' to detect the intrusion. The outcome of tanh activation function is mathematically evaluated as below,

$$A(F) = \begin{cases} \text{if } b(S_i) == b(SA), \text{ then } r(t) = +1 \\ \text{if } b(S_i) == b(WA), \text{ then } r(t) = -1 \\ \text{if } b(S_i) \neq b(SA) \text{ and } b(WA), \text{ then } r(t) = 0 \end{cases} \quad (3)$$

From (3), tanh activation function analyze the behavior of each sensor node ' $b(S_i)$ ' by comparing it with Sybil attack node behaviour ' $b(SA)$ ' and wormhole attack node behaviour ' $b(WA)$ ' to efficiently detect the intrusion is healthcare WSN. If the behaviour of sensor node is matched with Sybil attack node behaviour ' $b(SA)$ ', tanh activation function returns ' $+1$ ' as output which represents detection of Sybil attack node in healthcare WSN. If the behaviour of senor node is matched with wormhole attack node behaviour ' $b(WA)$ ', tanh activation function produces ' -1 ' which indicates a detection of wormhole attack node in healthcare WSN. If the behaviour of senor node is not matched with Sybil attack node behaviour and wormhole attack node behaviour, tanh activation function generates ' 0 ' as output which denotes a normal sensor node. The result of tanh activation function is demonstrated in below.

Figure 5 Result of Tanh Activation Function

Figure 5 presents the output of tanh activation function. As shown in the above figure, tanh activation function is an S-shaped curve. With help of tanh activation function, **tanh activation function** obtains the intrusion detection result in hidden layers. After finding the intrusion detection result, hidden layer sends it to the output layer. The activity of neurons in the output layer ' $w(t)$ ' at a time ' t ' is determined as,

$$r(t) = w_{qr} q_i(t) \quad (4)$$

From (4), ' w_{qr} ' signifies the weight between the hidden and output layer. The results of output layer at a time ' t ' mathematically determined as below,

$$r(t) = \begin{cases} +1 \rightarrow S_i \text{ is sybil attack node} \\ -1 \rightarrow S_i \text{ is wormhole attack node} \\ 0 \rightarrow S_i \text{ is normal node} \end{cases} \quad (5)$$

From (5), ' $r(t) = +1$ ' signifies that the sensor node ' S_i ' is a Sybil attack whereas ' $r(t) = -1$ ' points out that the sensor node ' S_i ' is a wormhole attack and ' $r(t) = 0$ ' represents that the sensor node ' S_i ' is a normal node in healthcare WSN. For each obtained result, the error function is then measured to increase the intrusion detection performance. On the contrary to existing works, Delta Ruled First Order Iterative Deep Learning employs mean square weighted deviation (MSWD) with the aim of significantly determining error function involved during the process of attack detection in a wireless network. The MSWD is a chi-squared that computes weighted sum of squared deviations using below mathematical formulation,

$$Er \leftarrow \chi^2 = \sum_i \frac{(t_j - y_j)^2}{\sigma_i^2} \quad (6)$$

From (6), ' σ ' indicates a variance, ' t_j ' represents a target output whereas ' y_j ' is the actual output. In weighted least squares, the definition is often written in matrix notation using below mathematical expression,

$$\chi^2 = r^T w r \quad (7)$$

From (7), ' r ' represents the vector of residuals, ' w ' points out the weight matrix and ' T ' refers to the inverse of the input (diagonal) covariance matrix of observations. Subsequently, the weights are updated according to error function.

On the contrary to state-of-the-art works, delta rule is applied in DRFOIDL-ID Technique for updating the weights of the inputs to artificial neurons. For a neuron ' j ' with activation function, the delta rule for weight updation is mathematically formulated as,

$$\Delta w_{pq} = \alpha (t_j - y_j) S_i \quad (8)$$

From (8), ' Δw_{pq} ' represents an updated weight, ' α ' refers to a small constant called learning rate, ' t_j ' denotes a target output whereas ' y_j ' is an actual output. Here, ' S_i ' indicates an actual input (i.e. sensor nodes). The delta rule is derived to diminish the error function in the output of the neural network through gradient descent. Then, DRFOIDL-ID Technique estimates the partial derivative of error function with respect to each weight. For each weight ' Δw_{ij} ', this derivative is obtained using below mathematical representation,

$$\frac{\partial Er}{\partial w_{pq}} = \left(\frac{\partial \left(\frac{(t_j - y_j)^2}{\sigma_i^2} \right)}{\partial w_{pq}} \right) \quad (9)$$

Followed by, chain rule is employed to divide the above equation into two derivatives as below,

$$\frac{\partial Er}{\partial w_{pq}} = \left(\frac{\partial \left(\frac{(t_j - y_j)^2}{\sigma_i^2} \right)}{\partial w_{pq}} \right) \frac{\partial y_j}{\partial w_{pq}} \quad (10)$$

From (10), weight between input and hidden layer ' w_{pq} ' is updated based on measured error function ' Er '. Similarly, the weights on hidden layer and output layer is changed using below,

$$\frac{\partial Er}{\partial w_q} = \left(\frac{\partial \left(\frac{(t_j - y_j)^2}{\sigma_i^2} \right)}{\partial w_q} \right) \frac{\partial y_j}{\partial w_q} \quad (11)$$

$$\frac{\partial Er}{\partial w_{qr}} = \left(\frac{\partial \left(\frac{(t_j - y_j)^2}{\sigma_i^2} \right)}{\partial w_{qr}} \right) \frac{\partial y_j}{\partial w_{qr}} \quad (12)$$

From (11) and (12), the weights on hidden layer and output layer are updated. After that, DRFOIDL-ID Technique utilized Gradient descent to optimize the error function of attack detection in a wireless network. On the contrary to conventional works, Gradient descent is applied in DRFOIDL-ID Technique in order to find the minimum of an error function. The Gradient descent is a first-order iterative optimization algorithm that adjusts weights according to the error function. From that, error function of attack detection is optimized using Gradient descent which is formulated as,

$$r(t) = \sum_{i=1}^n \arg \min Er(t) \quad (13)$$

From (13), ' $r(t)$ ' denotes a final output where ' $\arg \min$ ' assists for DRFOIDL-ID Technique to identify minimal error function for accurately detecting the attacks in healthcare WSN.

The algorithmic process of Delta Ruled First Order Iterative Deep Learning is shown in below.

// Delta Ruled First Order Iterative Deep Learning Algorithm

Input: Number of Sensor Nodes ' $S_i = S_1, S_2, S_3 \dots S_n$ ' in Healthcare WSN

Output: Improved Attack Detection Rate

Step 1: Begin

Step 2: Neural network is initialized with random weights

Step 3: For each ' S_i '

Step 4: While (' $Er(t)$ ' is lower) do

Step 5: Input layer takes ' S_i ' as input and pass it to hidden layer using (1)

Step 6: Hidden layers deeply analyze ' S_i ' using (2) and (3)

Step 7: Output layer ' $r(t)$ ' produces final result using (4)

Step 8: Determine error function ' $Er(t)$ ' using (6)

Step 9: Update weights ' Δw_{pq} ', ' Δw_q ', ' Δw_{qr} ' using (10), (11), and (12)

Step 10: Find minimal error function using (13)

Step 11: End while

```

Step 12:   If ( $r(t) = 1$ ) then
Step 13:     ' $S_i$ ' is a sybil attack node
Step 14:   Else If ( $r(t) = -1$ ) then
Step 15:     ' $S_i$ ' is a wormhole attack node
Step 16:   Else If ( $r(t) = 0$ ) then
Step 17:     ' $S_i$ ' is a normal node
Step 18:   End If
Step 19: End For
Step 20: End

```

Algorithm 1 Delta Ruled First Order Iterative Deep Learning

Algorithm 1 depicts the step by step processes of Delta Ruled First Order Iterative Deep Learning. With the support of the above algorithmic process, DRFOIDL-ID Technique enhances the accuracy of Sybil and wormhole attack detection in healthcare WSN with minimal time utilization. Therefore, DRFOIDL-ID Technique improves the attack detection rate and reduces the false positive rate, attack detection time in healthcare WSN as compared to state-of-the-art works.

3.3 Attacks Isolation Phase

After detecting the Sybil and wormhole attack nodes, the DRFOIDL-ID Technique accomplishes an attack isolation process to remove the intrusion nodes in healthcare WSN. During the attack isolation process, DRFOIDL-ID Technique broadcasts the isolation message to all sensor nodes in healthcare WSN and thereby separates the Sybil and wormhole attack nodes. The attack isolation process is presented in below

Figure 6 Process of attack isolation in healthcare WSN

Figure 6 depicts the attack isolation process to keep away Sybil and wormhole attack nodes from healthcare WSN. From figure, the arrow indicates the efficient route path selected for data transmission whereas dashed arrow denotes the broadcasting of isolation message to all sensor nodes in healthcare WSN. With the attack isolation process, DRFOIDL-ID Technique attains reliable data transmission with minimal packet loss. As a result, DRFOIDL-ID Technique improves the routing performance of healthcare WSN as compared to state-of-the-art works.

4. SIMULATION SETTINGS

To determine the performance, DRFOIDL-ID Technique is implemented in NS-2 simulator with network area of 1500 m*1500 m size using 500 sensor nodes. The simulation parameters are shown in below Table 1.

Table 1 Simulation Parameters

Simulation Parameters	Values
Simulator	NS2.34
Network area	1500 m * 1500 m
Number of sensor nodes	500
Mobility model	Random Waypoint model
Number of data packets	10,20,30,40,50,60,70,80,90,100
Speed of node	0 – 20 m/s
Simulation time	300s
Number of runs	10
Protocol	Dynamic Source Routing (DSR)

The performance of DRFOIDL-ID Technique is estimated in terms of attack detection rate, attack detection time, false positive rate and packet loss rate. The simulation result of DRFOIDL-ID Technique is compared with the existing two methods namely energy trust system (ETS) [1] and RPL-based wormhole detection mechanism [2].

5. RESULT AND DISCUSSIONS

In this section, the performance result of DRFOIDL-ID Technique is discussed. The efficiency of DRFOIDL-ID Technique is compared against with existing energy trust system (ETS) [1] and RPL-based wormhole detection mechanism [2] respectively. The effectiveness of DRFOIDL-ID Technique is determined along with the below metrics with the help of tables and graphs.

5.1 Performance Measure of Attack Detection Rate

Attack Detection Rate ‘ (ADR) ’ measures the ratio of number of sensor nodes that are correctly detected as Sybil or wormhole attacks to the total number sensor nodes. The attack detection rate is estimated using the relation below,

$$ADR = \frac{CD_{AN}}{T_{SN_i}} * 100 \quad (14)$$

From (14), the attack detection rate is determined. Here, ‘ T_{SN_i} ’ represents a total number of sensor nodes ‘ SN_i ’ and ‘ CD_{AN} ’ denotes a number of sensor nodes that are correctly detected as Sybil or wormhole attacks. The attack detection rate is evaluated in terms of percentages (%).

Sample Calculations:

- ❖ **Existing ETS:** number of sensor nodes correctly identified as Sybil or wormhole attacks is 35 and the total number of sensor node is 50. Then, the attack detection rate is evaluated as,

$$ADR = \frac{35}{50} * 100 = 70 \%$$

- ❖ **Existing RPL-based wormhole detection mechanism:** number of sensor nodes exactly detected as Sybil or wormhole attacks is 40 and the total number of sensor node is 50. Then, the attack detection rate is computed as,

$$ADR = \frac{40}{50} * 100 = 80 \%$$

- ❖ **Proposed DRFOIDL-ID Technique:** number of sensor nodes accurately predicted as Sybil or wormhole attacks is 46 and total number of sensor node is 50. Then, the attack detection rate is determined as,

$$ADR = \frac{46}{50} * 100 = 92 \%$$

In order to estimate the detection rate of Sybil and wormhole attack nodes in healthcare WSN, DRFOIDL-ID Technique is implemented in NS-2 simulator with a various number of sensor nodes in the range of 50-500. When employing the 350 sensor nodes for carry out the simulation evaluation, DRFOIDL-ID Technique gets 96 % attack detection rate whereas state-of-the-art works energy trust system (ETS) [1] and RPL-based wormhole detection mechanism [2] obtains 86 % and 89 % respectively. From that, it is illustrative that the attack detection rate using DRFOIDL-ID Technique is higher as compared to other works. The performance result analysis of attack detection rate is demonstrated in below.

Figure 7 Impacts of Attack Detection Rate versus Number of Sensor Nodes

Figure 7 presents the comparative result analysis of attack detection rate versus a different number of sensor nodes using three methods namely ETS [1] and RPL-based wormhole detection mechanism [2] and DRFOIDL-ID Technique. As exposed in above figure, DRFOIDL-ID Technique provides higher attack detection rate for finding the Sybil and wormhole attack nodes in healthcare WSN as compared to existing ETS [1] and RPL-based wormhole detection mechanism [2]. This is owing to application of mean square weighted deviation (MSWD) in Delta Ruled First Order Iterative Deep Learning on the contrary to existing works. With the application of MSWD, DRFOIDL-ID Technique significantly determines the error function during processes of Sybil and wormhole attack nodes detection. The accurate measurement of error function helps for DRFOIDL-ID Technique to improve the instruction detection performance as compared to existing works. This assists for DRFOIDL-ID Technique to enhance the ratio of number of sensor nodes that are correctly detected as Sybil or wormhole attacks. Hence, DRFOIDL-ID Technique increases the attack detection rate by 14 % and 9 % as compared ETS [1] and RPL-based wormhole detection mechanism [2] respectively.

5.2 Performance Result of Attack Detection Time

Attack detection time (ADT) estimates the amount of time taken to detect Sybil or wormhole attacks in WSN. The attack detection time is determined using below,

$$ADT = T_{SN_i} * T(DSA) \quad (15)$$

From (15), ' $T(DSA)$ ' point outs the time employed for single Sybil or wormhole attack node in the network and ' T_{SN_i} ' indicates a total number of sensor nodes. The attack detection time is estimated in terms of milliseconds (ms).

Sample Calculations:

- ❖ **Existing ETS:** time employed to find single Sybil or wormhole attacks is 0.44ms and total number of sensor nodes is 50. Then, the attack detection time is computed as,

$$ADT = 50 * 0.44 = 22 \text{ ms}$$

- ❖ **Existing RPL-based wormhole detection mechanism:** time utilized to identify single Sybil or wormhole attacks is 0.4 ms and total number of sensor nodes is 50. Then, the attack detection time is calculated as,

$$ADT = 50 * 0.40 = 20 \text{ ms}$$

- ❖ **Proposed DRFOIDL-ID Technique:** time consumed to detect single Sybil or wormhole attacks is 0.25 ms and total number of sensor nodes is 50. Then, the attack detection time is estimated as,

For evaluating the time complexity involved during identification of Sybil and wormhole attack nodes in healthcare WSN, DRFOIDL-ID Technique is implemented in NS-2 simulator by considering a different number of sensor nodes in the range of 50-500. ~~ADT = 50 * 0.25 = 13 ms~~ In taking the 405 sensor nodes for accomplishing simulation work, DRFOIDL-ID Technique acquires 60 ms attack detection time whereas conventional energy trust system (ETS) [1] and RPL-based wormhole detection mechanism [2] employs 76 ms and 68 ms respectively. From the above results, it is clear that the attack detection time using DRFOIDL-ID Technique is lower when compared to other works. The simulation result analysis of attack detection time is shown in below.

Table 2 Tabulation for Attack Detection Time

Number of Sensor Nodes	Attack Detection Time (ms)		
	ETS	RPL-based wormhole detection mechanism	DRFOIDL-ID Technique
50	22	20	13
100	37	35	20
150	36	33	29
200	46	42	26
250	55	50	45
300	63	57	51
350	70	63	56
400	76	68	60
450	81	72	59
500	85	75	65

Table 2 describes the performance result analysis of attack detection time versus a varied number of sensor nodes using three methods namely ETS [1] and RPL-based wormhole detection mechanism [2] and DRFOIDL-ID Technique. As presented in above table, DRFOIDL-ID Technique provides lower attack detection time for discovering the Sybil and wormhole attack nodes in healthcare WSN when compared to existing ETS [1] and RPL-based wormhole detection mechanism [2]. This is due to the application of delta rule in DRFOIDL-ID Technique on the contrary to state-of-the-art works. By using the delta rule, DRFOIDL-ID Technique determines the derivative of the network's weights with respect to the output error and also adjusts the weights to accurately detect the intrusions

in healthcare WSN with minimal time. This supports for DRFOIDL-ID Technique to utilize the amount of time taken to identify Sybil or wormhole attacks in WSN. Thus, DRFOIDL-ID Technique reduces the attack detection time by 28 % and 20 % as compared ETS [1] and RPL-based wormhole detection mechanism [2] respectively.

5.3 Performance Result of False Alarm Rate

False Alarm Rate ' (FAR) ' estimates the ratio of number of sensor nodes that are incorrectly detected as Sybil or wormhole attack to the total number of sensor nodes. The false alarm rate is calculated as,

$$FAR = \frac{ID_{AN}}{T_{SN_i}} * 100 \quad (16)$$

From (16), false alarm rate of intrusion detection is evaluated. Here, ' T_{SN_i} ' refers to a total number of sensor nodes ' SN_i ' and ' ID_{AN} ' signifies a number of sensor nodes that are incorrectly detected as Sybil or wormhole attack. The false alarm rate is determined in terms of percentages (%).

Sample Calculations:

- ❖ **Existing ETS:** number of sensor nodes inaccurately predicted as Sybil or wormhole attacks is 15 and the total number of sensor node is 50. Then, the false alarm rate is formulated as,

$$FAR = \frac{15}{50} * 100 = 30 \%$$

- ❖ **Existing RPL-based wormhole detection mechanism:** number of sensor nodes incorrectly identified as Sybil or wormhole attacks is 10 and total number of sensor node is 50. Then, the false alarm rate is obtained as,

$$FAR = \frac{10}{50} * 100 = 20\%$$

- ❖ **Proposed DRFOIDL-ID Technique:** number of sensor nodes inexactly detected as Sybil or wormhole attacks is 4 and total number of sensor node is 50. Then, the false alarm rate is computed as,

$$FAR = \frac{4}{50} * 100 = 8 \%$$

To measure the false alarm rate of Sybil and wormhole attack detection in healthcare WSN, DRFOIDL-ID Technique is implemented in NS-2 simulator using a diverse number of sensor nodes in the range of 50-500. When conducting the simulation process using 300 sensor nodes, DRFOIDL-ID Technique attains 28 % false alarm rate whereas existing energy trust system (ETS) [1] and RPL-based wormhole detection mechanism [2] obtains 55 % and 40 % respectively. Accordingly, it is significant that the false alarm rate using DRFOIDL-ID Technique is minimal as compared to other works. The comparative result analysis of false alarm rate is explained in below.

Figure 8 Impacts of False Alarm Rate versus Number of Sensor Nodes

Figure 8 portrays the performance result analysis of false alarm rate versus a diverse number of sensor nodes using three methods namely ETS [1] and RPL-based wormhole detection mechanism [2] and DRFOIDL-ID Technique. As shown in above figure, DRFOIDL-ID Technique provides minimal false alarm rate in order to detect the Sybil and wormhole attack nodes in healthcare WSN when compared to existing ETS [1] and RPL-based wormhole detection mechanism [2]. This is because of the application of first order iterative optimization algorithm in DRFOIDL-ID Technique on the contrary to conventional work. With the support of first-order iterative optimization algorithm, DRFOIDL-ID Technique determines the optimal weight that minimizes error function to detect the Sybil and wormhole attack nodes in healthcare WSN without any false. This helps for DRFOIDL-ID Technique to reduces the ratio of number of sensor nodes that are incorrectly detected as Sybil or wormhole attack. Therefore, DRFOIDL-ID Technique decreases the false alarm rate by 61 % and 52 % as compared ETS [1] and RPL-based wormhole detection mechanism [2] respectively.

5.4 Performance Result of Packet Loss Rate

Packet Loss Rate ‘(PLR)’ determines the number of data packets dropped during transmission to the total number of packets sent. The packet loss rate is evaluated using below,

$$PLR = N_{DP} - T_{DP} \quad (17)$$

From equation (17), packet loss during data transmission is obtained. Here, ‘ N_{DP} ’ indicates a total number of data packets and ‘ T_{DP} ’ refers a number of data packets that are successfully delivered at destination. The packet loss rate is estimated in terms of packets per second (pps).

Sample Calculations:

- ❖ **Existing ETS:** number of data packets successfully delivered at the destination is 4 and the total number of data packets is 10. Then, the packet loss rate is measured as,

$$PLR = 10 - 4 = 6 \text{ pps}$$

- ❖ **Existing RPL-based wormhole detection mechanism:** number of data packets successfully reached at destination is 5 and total number of data packets is 10. Then, the packet loss rate is estimated as,

$$PLR = 10 - 5 = 5 \text{ pps}$$

- ❖ **Proposed DRFOIDL-ID Technique:** number of data packets successfully sent to destination is 8 and total number of data packets is 10. Then, the packet loss rate is determined as,

$$PLR = 10 - 8 = 2 \text{ pps}$$

The DRFOIDL-ID Technique is implemented in NS-2 simulator with help of a different number of data packets in the range of 10-100 to calculate the packet loss rate in healthcare WSN. When performing the simulation work using 50 data packets, DRFOIDL-ID technique obtains 11 % packet loss rate whereas state-of-the-art works energy trust system (ETS) [1] and RPL-based wormhole detection mechanism [2] gets 25 % and 20 % respectively. Thus, it is observed that the packet loss rate using DRFOIDL-ID technique is very lower as compared to other works. The tabulation result analysis of packet loss rate is depicted in below.

Table 3 Tabulation for Packet Loss Rate

Number of data packets	Packet Loss Rate (pps)		
	ETS	RPL-based wormhole detection mechanism	DRFOIDL-ID Technique
10	6	5	2
20	16	11	4
30	18	13	7
40	23	18	11
50	25	20	10
60	31	25	18
70	29	24	20
80	35	30	23
90	38	33	27
100	45	38	31

Table 3 depicts the simulation result analysis of packet loss rate versus a different number of data packets using three methods namely ETS [1] and RPL-based wormhole detection mechanism [2] and DRFOIDL-ID technique. As exposed in the above table, DRFOIDL-ID technique provides a lower packet loss rate for data transmission in healthcare WSN when compared to existing ETS [1] and RPL-based wormhole detection mechanism [2]. This is due to designing of Delta Ruled First Order Iterative Deep Learning in DRFOIDL-ID technique on the contrary to existing works. With the algorithmic processes of Delta Ruled First Order Iterative Deep Learning, DRFOIDL-ID technique finds the Sybil and wormhole attacks in healthcare WSN. Consequently, DRFOIDL-ID technique eliminates the Sybil and wormhole attacks in healthcare WSN by sending the isolation messages. This assists for DRFOIDL-ID Technique to perform effective data delivery in healthcare WSN. Hence, DRFOIDL-ID Technique reduces the number of packets dropped during data transmission. As a result, DRFOIDL-ID Technique minimizes the packet loss rate by 48 % and 36 % as compared ETS [1] and RPL-based wormhole detection mechanism [2] respectively.

6. CONCLUSION

The DRFOIDL-ID Technique is developed with goal of improving the Sybil and wormhole attacks detections performance to attain efficient routing in healthcare WSN. The goal of DRFOIDL-ID technique is achieved with application of Delta Ruled First Order Iterative Deep Learning. With support of Delta Ruled First

Order Iterative Deep Learning algorithmic processes, DRFOIDL-ID technique efficiently discovers the Sybil and wormhole attack nodes in healthcare WSN with minimal time consumption. Then, DRFOIDL-ID technique avoids the discovered Sybil and wormhole attack nodes by means of distributing the isolation message to all sensor nodes in healthcare WSN to decrease loss rate. As a result, DRFOIDL-ID technique achieves reliable data delivery in healthcare WSN. The performance of DRFOIDL-ID technique is determined in terms of attack detection rate, attack detection time, packet loss rate and false alarm rate and compared with existing two methods. The simulation result demonstrates that the DRFOIDL-ID technique offers better performance with enhancement of attack detection rate and minimization of attack detection time as compared to state-of-the-art works.

Author Declaration Form

I declare that:

Title of Manuscript: DELTA RULED FIRST ORDER ITERATIVE DEEP NEURAL LEARNING FOR SYBIL AND WORMHOLE ATTACKS DETECTION IN HEALTHCARE WIRELESS SENSOR NETWORK

We author(s) of the above titled paper hereby declare that the work included in the above paper is original and is an outcome of the research carried out by the authors indicated in it. Further, We author(s) declare that the work submitted for wireless personal communications has not been published already or under consideration for publication in any Journals/Conferences/Symposia/Seminars.

**Yours Sincerely,
A. John Clement Sunder**

**Associate Professor, ECE,
Bannari Amman institute of Technology
Sathyamangalam,
Tamil Nadu, India,
E-mail: sundarajcece@gmail.com**

***Funding : Not Applicable**

***Conflicts of interest : John Clement Sunder declares that he has no conflict of interest.**

***Availability of data and material (data transparency) : Not Applicable**

***Code availability (software application or custom code) : Not Applicable**

REFERENCES

- [1] Alsaedi, N., Hashim, F., Sali, A. and Rokhani, F.Z., 2017. Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS). *Computer Communications*, 110, pp.75-82.
- [2] Lai, G.H., 2016. Detection of wormhole attacks on IPv6 mobility-based wireless sensor network. *EURASIP Journal on Wireless Communications and Networking*, 2016(1), p.274.
- [3] Dong, W. and Liu, X., 2015. Robust and secure time-synchronization against sybil attacks for sensor networks. *IEEE Transactions on Industrial Informatics*, 11(6), pp.1482-1491.

- [4] Al-Qurishi, M., Alrubaian, M., Rahman, S.M.M., Alamri, A. and Hassan, M.M., 2018. A prediction system of Sybil attack in social network using deep-regression model. *Future Generation Computer Systems*, 87, pp.743-753.
- [5] Amish, P. and Vaghela, V.B., 2016. Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. *Procedia computer science*, 79, pp.700-707.
- [6] Yuan, Y., Huo, L., Wang, Z. and Hogrefe, D., 2018. Secure APIT Localization Scheme Against Sybil Attacks in Distributed Wireless Sensor Networks. *IEEE Access*, 6, pp.27629-27636.
- [7] Khalil, I., Bagchi, S. and Shroff, N.B., 2007. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Computer networks*, 51(13), pp.3750-3772.
- [8] Wen, M., Li, H., Zheng, Y.F. and Chen, K.F., 2008. TDOA-based Sybil attack detection scheme for wireless sensor networks. *Journal of Shanghai University (English Edition)*, 12(1), pp.66-70.
- [9] Bhise, A.M. and Kamble, S.D., 2016. Review on Detection and Mitigation of Sybil Attack in the Network. *Procedia Computer Science*, 78, pp.395-401.
- [10] Saud Khan, M. and Khan, N.M., 2016. Low complexity signed response based sybil attack detection mechanism in wireless sensor networks. *Journal of Sensors*, 2016.
- [11] Shipra Diwakar, R. Kashyup., 2017. Detecting Sybil Attack Using Hybrid Fuzzy K-Means Algorithm in WSN. *International Journal of Engineering Development and Research*, 5(2), pp 1560-1565.
- [12] Dhamodharan, U.S.R.K. and Vayanaperumal, R., 2015. Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, 2015.
- [13] Kaur, M. and Jethi, M.A., 2017. Sybil Attack in Wireless Sensor Networks: A Survey.
- [14] Almas Shehni, R., Faez, K., Eshghi, F. and Kelarestaghi, M., 2017. A New Lightweight Watchdog-Based Algorithm for Detecting Sybil Nodes in Mobile WSNs. *Future Internet*, 10(1), p.1.
- [15] Palak. 2017. Fuzzy based Sybil attack detection in Wireless Sensor Network. *International Journal of Computer Sciences and Engineering*, 5(11), pp 50-56.
- [16] Sookhak, M., Akhundzada, A., Sookhak, A., Eslaminejad, M., Gani, A., Khan, M.K., Li, X. and Wang, X., 2015. Geographic wormhole detection in wireless sensor networks. *PloS one*, 10(1), p.e0115324.
- [17] Sarigiannidis, P., Karapistoli, E. and Economides, A.A., 2015. Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. *Expert Systems with Applications*, 42(21), pp.7560-7572.
- [18] Singh, R., Singh, J. and Singh, R., 2016. TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 16(11), p.90.
- [19] Ramachandran, S. and Shanmugan, V., 2011. Impact of sybil and wormhole attacks in location based geographic multicast routing protocol for wireless sensor networks. *Journal of Computer Science*, 7(7), p.973.
- [20] Xiao, L., Greenstein, L.J., Mandayam, N.B. and Trappe, W., 2009. Channel-based detection of sybil attacks in wireless networks. *IEEE Transactions on Information Forensics and Security*, 4(3), pp.492-503.

Figures

Figure 1

Example of Wormhole Attack in Healthcare WSN

Figure 2

an Example of Sybil Attack in Healthcare WSN

Figure 3

Architecture Diagram of DRFOIDL-ID Technique for Sybil and Wormhole Attack Detection and Isolation

Figure 4

Process of Delta Ruled First Order Iterative Deep Learning for Intrusion Detection

Figure 5

Result of Tanh Activation Function

Figure 6

Process of attack isolation in healthcare WSN

Figure 7

Impacts of Attack Detection Rate versus Number of Sensor Nodes

Figure 8

Impacts of False Alarm Rate versus Number of Sensor Nodes