International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212334 Volume 9, Issue 2, March – April (2022)

RESEARCH ARTICLE

Performance Analysis of Malicious Node Detection in Wireless Multimedia Sensor Networks using Modified LeNET Architecture

S. Arockia Jayadhas
Faculty of Electronics, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India
dhasjohn85@gmail.com

S. Emalda Roslin
Department of ECE, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India
roemi_mich@yahoo.co.in

Received: 14 January 2022 / Revised: 04 March 2022 / Accepted: 11 March 2022 / Published: 30 April 2022

Abstract – The routing performance in Wireless Multimedia Sensor Network (WMSN), which transfers and receives multimedia content like a scalar, audio and video, is often affected by malicious nodes and residual nodes. An external attacker modifies the characteristics function of the node, and thus the node becomes malicious nodes in WMSN. These malicious nodes will affect the functionalities of its surrounding nodes and prevent routing through it and other nodes. Hence, the detection and mitigation of malicious nodes are essential to improve the routing efficiency in WMSN. The conventional methods mainly used machine learning algorithms to identify the malicious nodes in WMSN, which provided low accuracy and consumed more detection time as the main drawbacks. The proposed methodology resolves these drawbacks of the conventional algorithms in this paper. This paper presents an efficient method for detecting and mitigating the malicious nodes using feature index, which is optimized by a Genetic Algorithm (GA). The optimized feature set is classified by the modified LeNET deep learning classification approach. Even though conventional deep learning architectures provide a high classification rate for malicious node detection, it consumes a high detection time to identify malicious nodes. This drawback is overcome by modifying the internal layers of the existing LeNET architecture into parallel, and the dense layers in the existing LeNET architecture are replaced by Fuzzy C Means (FCM) algorithm. The performance of the proposed methodology is analyzed with respect to misclassification rate, precision, recall, accuracy and F1-score parameters.

Index Terms – Wireless Multimedia Sensor Network, Malicious Node, Detection, Mitigation, Classification, Genetic Algorithm, FCM.

1. INTRODUCTION

Wireless Multimedia Sensor Network (WMSN) is a type of WSN mainly concentrated on transferring or receiving multimedia information such as scalar, audio, and video signals. The nodes in WMSN also transmit and receive the scalar data such as temperature, pressure and humidity. Wireless Sensor Networks (WSN) is a wireless network that collects surrounding environment information through sensor nodes. This WSN consists of several sensor nodes, central unit (cluster head) and base station [1-3]. Each sensor node is equipped with a sensing element, analog to digital converter unit and transmission section. The sensing element in each sensor node senses the various metrics in the surrounding environment, and this sensed analog information is converted into digital data [4-5]. This converted digital data is transmitted to the nearby sensor or cluster head by transmission section. Apart from WSN, the nodes in WMSN consume high energy for multimedia data transmission and reception due to its extensive data [6]. Hence, WMSN is important when compared with WSN. Figure1 shows the architecture of WMSN. This network consists of a data acquisition unit, the compressive sensing element and the transmitter section, which transmits the sensed information to the cluster head of the network [7]. The non-linear functionality and power dependency are the main characteristics of the nodes in WMSN.

The current methodologies such as data fusion algorithm, stereo matching algorithm and multimedia sensing coverage protocol model are used for analyzing the performance of the sensor node architecture. The main problem of this high energy consumption is solved by detecting the malicious behaviour sensor nodes in WMSN. The detection of malicious behaviour sensor nodes among the set of sensor nodes is a complex task due to its similar characters with normal sensor nodes in multimedia networks [8]. Also, the malicious nodes create dummy packets and send them to all of their surrounding nodes to degrade their functional activities. The performance of the WMSN is highly dependent on the detection and mitigation of these kinds of

RESEARCH ARTICLE

malicious nodes in the WMSN environment. Hence, this paper proposes a methodology to detect the malicious behaviour sensor nodes in the WMSN environment.

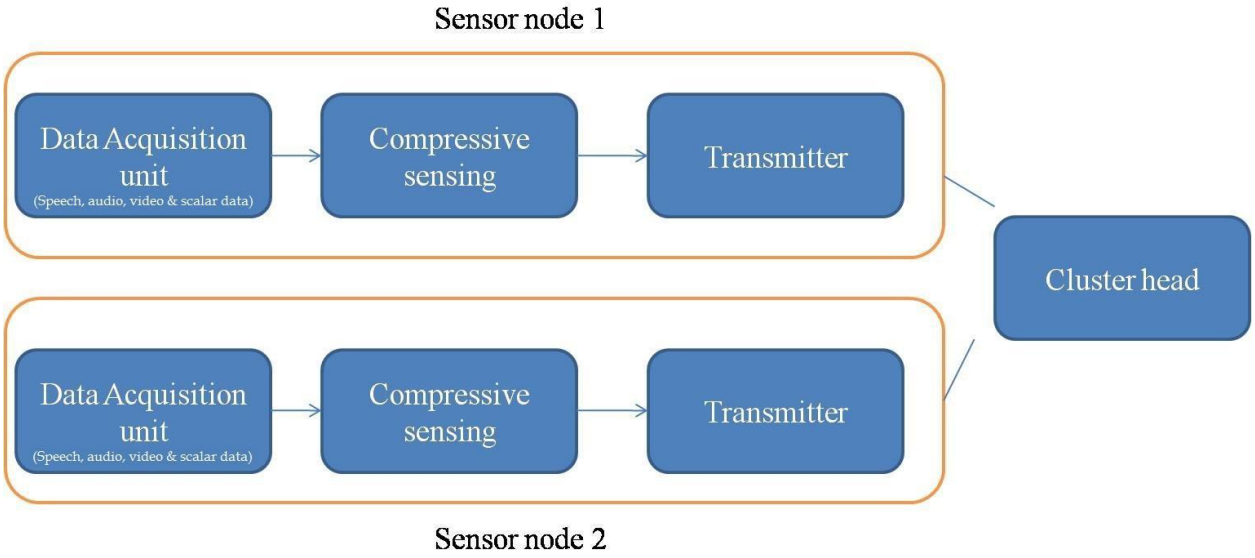

Figure 1 Wireless Multimedia Sensor Network

The research objectives of this paper are stated below:

- To propose a novel deep learning architecture for the detection of malicious nodes in the WMSN environment.
- To improve the malicious node detection rate.
- To reduce the malicious node detection time.

In this paper, the LeNET architecture identifies the malicious sensor nodes in WMSN. This LeNET architecture consists of Convolutional layers, pooling layers and dense layers. The function of the Convolutional layer is to convolve the input parameter with its corresponding Convolutional filter to produce the internal feature values. The size of these internal feature values is minimized using pooling layers placed at the end of every Convolutional layer. All the internal features are fed into dense layers to produce the linear binary output, which corresponds to the final classification results.

The statement of the research problem is given as follows:

- There is a need for detecting the malicious sensor nodes in the WMSN environment in order to improve the performance efficiency.
- Even though much conventional deep learning architecture is available to detect malicious nodes in the WMSN environment, the detection time is high due to its complex architecture design. These problems are solved by proposing the modified LeNET architecture in this paper for detecting malicious nodes.

The conventional problems and their solutions are depicted in section 2, the proposed methodology and its concepts are illustrated in section 3. Section 4 discusses the results and their impact on WMSN, and section 5 concludes this paper.

2. LITERATURE SURVEY

Jin et al. [1] developed wireless multimedia networks using Zigbee core architecture in each sensor node in a network environment. The authors used an improved Census transform stereo matching algorithm for improving the performance of the wireless multimedia networks with respect to energy consumption optimization. The authors obtained a 72% of precision rate for their proposed method implementation.

Zhiming Zhang et al. [9] detected and identified the location of malicious sensor nodes in wireless sensor networks using a Homomorphic security algorithm. The authors discussed the effectiveness of the proposed homomorphic algorithm with respect to different sensor nodes segments. Ramasamy et al. [10] stated many conventional algorithms and methodologies for detecting the malicious nodes in wireless sensor networks. The limitations and novelties of each conventional method were discussed in this work.

Alzubaidi et al. [11] used a conventional LeNET algorithm to identify each sensor node's malicious and suspicious activities in WMSN. The limitation of this work was that this method consumed more time for identifying the malicious activities of the sensor nodes. Koyuncu et al. [12] used a data fusion algorithm to construct wireless multimedia networks with an audio and visual model. The authors developed this linear energy-efficient model architecture for object recognition in large sensor wireless networks. The authors obtained an

RESEARCH ARTICLE

89.7% of precision rate along with an 89.9% of recall rate for their proposed design methodology.

Ahmed Salim et al. [13] constructed Coverage Model and Cover Set method for performance improvement in the WMSN environment. Each node followed certain cover set rules for developing a coverage model. The authors finally analyzed the performance of the proposed system with respect to various simulation parameters. Based on the developed coverage model, a scheduling algorithm was developed for allocating the period for node multimedia data transmission.

Harsh Bhatt et al. [14] detailed various conventional methodologies for developing an efficient architecture of WMSN. The author analyzed design methodologies and parameter selection for improving the network model environment. Pournazari et al. [15] constructed a multimedia sensing coverage protocol model for improving the performance of multimedia networks. The authors developed prioritizing table for each node in multimedia networks, and based on this priority table, the nodes' data transmission was started. The authors obtained a 92.7% of precision rate and 91.7% of recall rate for their proposed design methodology.

Li W. [16] used Particle Swarm Optimization (PSO) algorithm for optimizing the computed features from all the features in wireless sensor networks. The authors discussed the complexity of this algorithm in this paper. Domínguez-Medina et al. [17] used the Ant Colony Optimization (ACO) algorithm to optimize the computed features from all the features in wireless sensor networks. The complexity of this algorithm was discussed by the authors in this paper. The structure of this ACO algorithm was fixed with respect to the size of the fitness function.

The drawbacks of previous works are stated below:

- Most of the existing methods are not implementing any soft computing based machine learning approaches to detect malicious nodes.
- The classification rate performance was not optimum.
- The detection time of the malicious node was high.

The advantages of the proposed method are stated as:

- The proposed method stated in this paper uses soft computing based deep learning approaches (modified LeNET) for the detection of malicious nodes.
- The classification rate performance is high using GA.

The novelty of the proposed method is stated as:

The internal layers of the existing LeNET architecture are modified into parallel, and the dense layers in the existing LeNET architecture are replaced by Fuzzy C Means (FCM) algorithm. This improves the malicious node classification accuracy and reduces the malicious node detection time significantly compared with the conventional LeNET architecture for the malicious node detection process.

3. MALICIOUS NODE DETECTION USING GA AND MODIFIED DEEP LEARNING ALGORITHM

This paper proposes an efficient methodology for detecting and mitigating the malicious nodes using feature index, which is optimized by a Genetic Algorithm (GA). The optimized feature set is classified by the modified LeNET classification approach. This classifier classifies every node in wireless multimedia sensor networks into either malicious node or non-malicious node based on the trained feature set. The proposed flow for malicious sensor node detection in WMSN is illustrated in Figure 2.

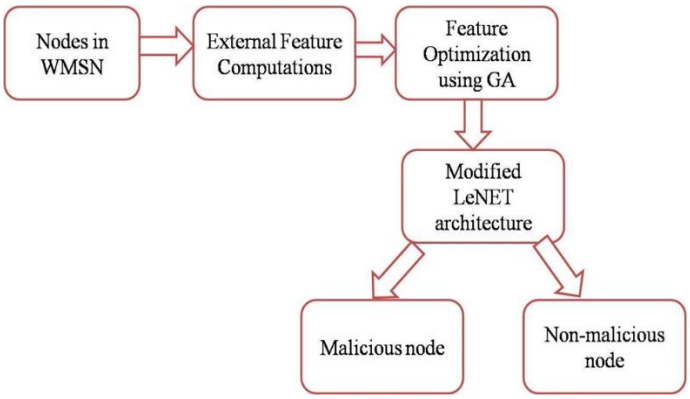

Figure 2 Malicious Node Detection in Wireless Multimedia Sensor Networks

3.1. Feature Extraction

Every sensor node in the WMSN environment has a unique feature with respect to its surrounding or nearby sensor nodes. This will be used to detect the malicious and non-malicious sensor nodes in WMSN. In this paper, Mutual Information, Redundancy metric and distance metric are computed for every node to be tested and its surrounding sensor nodes in the WMSN environment.

3.2. Mutual Information

Mutual Information (MI) is defined as the information required between two or more sensor nodes to perform mutual coupling in order to improve the relativity rate. MI feature index metric is computed between the node to be tested and its nearby node in WMSN. The computed MI is used as the feature property between the sensor nodes for the classification of the sensor node. The value of the computed MI lies below 100. This MI feature value determines the sensor node behaviour in WMSN. The malicious sensor node has a low MI feature value, and the non-malicious sensor node has a high MI feature value. If the value of MI is high (greater than 80), the node is initially classified as a non-

RESEARCH ARTICLE

malicious node, indicating a high level of certainty between two sensor nodes. If the value of MI is low (less than 80), the node is initially classified as a malicious node which indicates that there is a low level of certainty between two sensor nodes.

The MI is computed between two nearby nodes in WMSN is given in equation (1),

$$MI(node1, node2) = \sum_{x=1}^{\infty} \sum_{y=1}^{\infty} P(x,y) * log \frac{P(x,y)}{P(x)*P(y)} \quad (1)$$

Whereas node 1(x) represents the node to be tested and node 2 (y) represents the nearby node in the WMSN environment. The nodes' energy level is represented by P(x) and P(y).

In this paper, the node's initial energy level is set to 1000 J, and it is gradually decreased with respect to the time period.

3.1.2. Redundancy Metric

The redundancy feature of the sensor node shows its efficiency in terms of its behaviour metric. The redundancy metric shows the relation between the node to be tested and all of its surrounding nodes in WMSN. This feature metric is computed between the node to be tested in WMSN and all of its surrounding nodes [18]. The redundancy feature value must be below, which indicates that there is a low level of redundancy present between the sensor nodes. The value of the redundancy feature varies between 0 and 1. The malicious sensor node has a high value of redundancy feature (more than 0.8), and the non-malicious sensor node has a low value of the redundancy feature (less than 0.8).

This metric can be computed using the following equation (2).

$$Redundancy\ metric = \frac{1}{S^2} * \sum_{i=1}^{N} P(x) * P(y_i) \quad (2)$$

Whereas S is the scaling factor and is determined using equation (3) in equation (2).

$$S = \frac{P(x)+\sum_{i=1}^{N} P(y_i)}{P(x)} \quad (3)$$

Whereas N is the number of surrounding nodes around the node to be tested.

3.1.3. Distance Metric

The sensor nodes are slowly moving in the WMSN environment during the data transmission and reception process. The movement of these sensor nodes is measured by computing its distance metric. The computation of the distance between the node to be tested and its surrounding node in WMSN is essential for malicious node detection. The distance metrics [19-20] between the node to be tested and its surrounding sensor nodes are computed and updated in the distance metric matrix. After 't' seconds, the distance metric matrix is updated by computing the new distance metric between the sensor nodes. The deviation between the previous and recently updated distance metrics are computed, which determines the behaviour of the sensor node. If this computed distance metric varies abruptly with all of its surrounding nodes, then the tested node is identified as a dynamic node, and it is assumed to be a malicious node. If this computed distance metric varies slightly with all of its surrounding nodes, then the tested node is identified as the static node and assumed to be a non-malicious node.

Figure 3 shows the distance metric computation between nodes in WMSN.

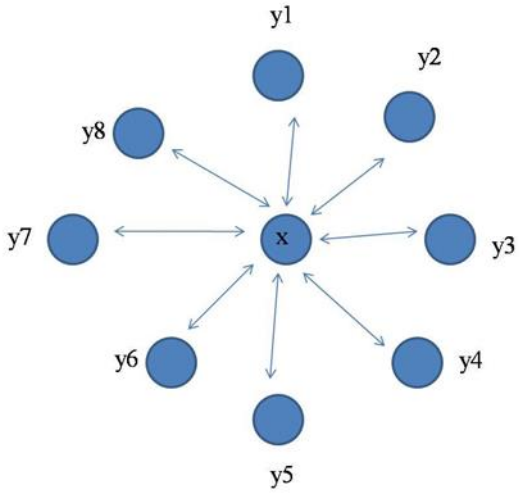

Figure 3 Distance Metric Computation between Nodes in WMSN

The distance metric with respect to the spatial domain is computed between the node to be tested and its surrounding nodes, and it is given in the following equation (4),

$$D_{spatial} = \sum_{i=1}^{N} \frac{|x-y_i|}{|x|+|y_i|} \quad (4)$$

The distance metric with respect to frequency domain is computed between the node to be tested and its surrounding nodes, and it is given in the following equation (5),

$$D_{freequency} = \sum_{i=1}^{N} |x - y_i| \quad (5)$$

The final distance metric is determined using its spatial domain distance metric and frequency domain distance metric, and it is given in the following equation (6) using the equations (4) and (5).

$$Distancemetric = \frac{Dist_{spatial} - Dist_{frequency}}{Dist_{frequency}} \quad (6)$$

The extracted features from each sensor node in the WMSN environment is optimized using the optimization algorithm Genetic approach [21]. In this paper, the Lagrange multiplier method is used to compute the fitness function of GA. The problem is to find the best-computed feature from the feature

RESEARCH ARTICLE

vector for Mutual information (x), Redundancy metric (y) and Distance metric (z) so that their total value is equal to a value t. The main aim of the fitness function is to reduce the sum x+y+z from deviating from t, i.e. |x + y + z — t| should be zero. Hence the fitness function can be considered as the inverse of |x + y + z - t|.

The GA used in this paper is explained with the following steps:

Step 1:

Set the computed features in Chromosome 1 (CHR1) and Chromosome 2 (CHR2).

Step 2:

Find the Euclidean Distances (ED) of all the elements in both CHR1 and CHR2.

Step 3:

Find the minimum value of the computed EDs, and the minimum values are noted as M1 and M2.

Step 4:

The CHR1 is fixed, and the elements in CHR2 are refilled with the following feature elements if M1 is greater than M2.

Step 5:

The CHR2 is fixed, and the elements in CHR1 are refilled with the next feature elements if M2 is greater than M1.

This approach selects the best features from the large set of available features from each sensor node in multimedia networks. The optimized features will be classified further using the classification technique.

3.2. Classifications

In this paper, deep learning architecture (Rinki Gupta et al. [22]) is used to detect the malicious sensor nodes in the WMSN environment based on the optimized features which are extracted from the sensor node using its energy level.

The Optimized Feature Maps (OFM) from the GA process is classified into either malicious or non-malicious nodes using deep learning architecture in this work. There are numerous deep learning architectures available for the classification process. Among them, LeNET deep learning architecture is the simple architecture that contains minimum numbers of Convolutional Layers (Conv_Layer) and Pooling Layers (Pool_Layer) with Dense Layers (Dense_Layer), as illustrated in Figure 5(a). Even though this architecture provides a high classification rate for malicious node detection, it consumes a high detection time for the identification of malicious nodes. This drawback is overcome by modifying the internal layers of the existing LeNET architecture into parallel, and the dense layers in the existing LeNET architecture are replaced by Fuzzy C Means (FCM) algorithm, as illustrated in Figure 5(b).

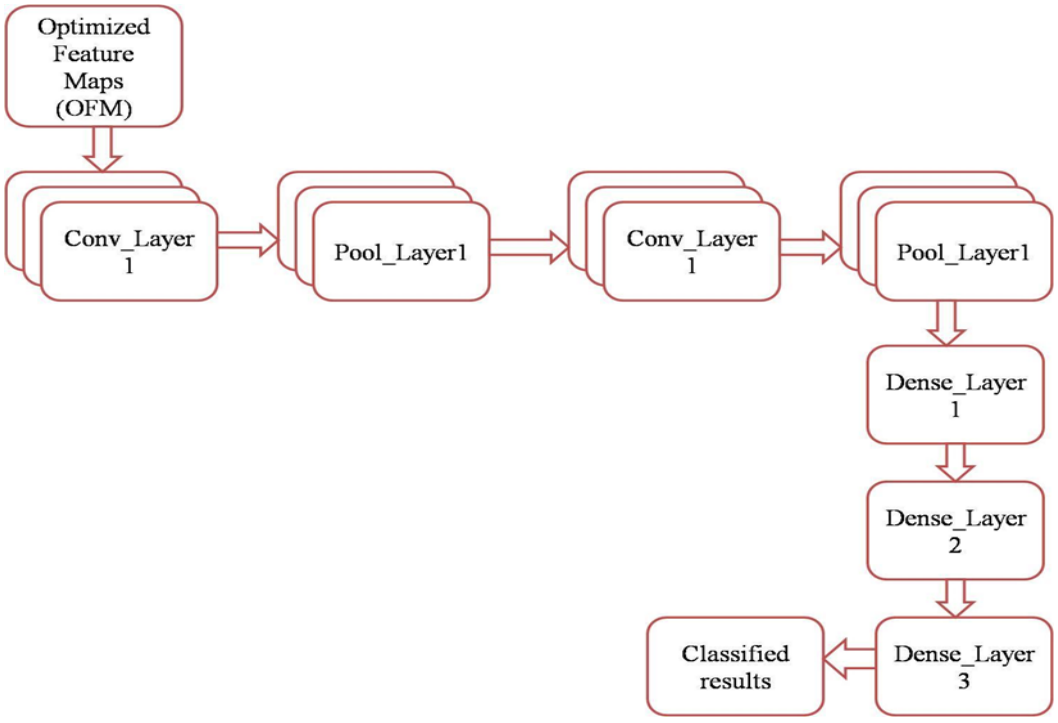

Figure 5 (a) Existing LeNET Deep Learning Architecture

RESEARCH ARTICLE

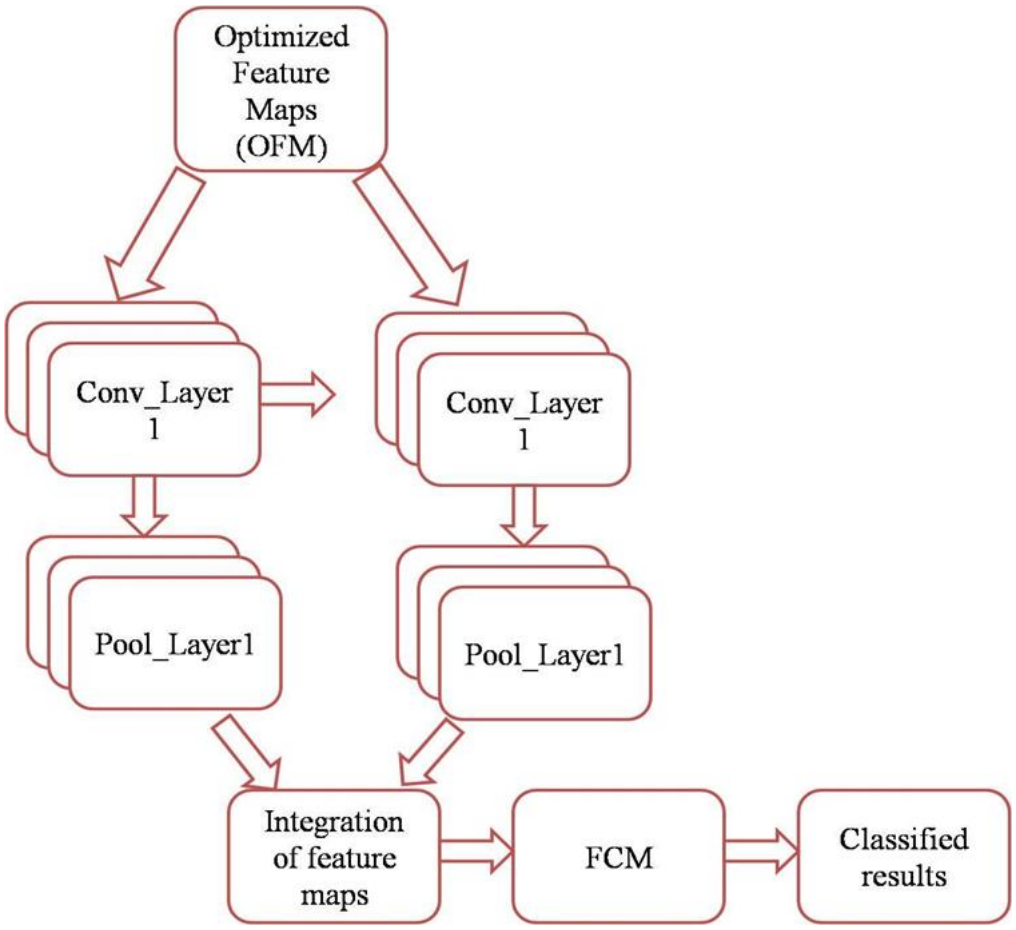

Figure 5(b) Proposed LeNET Architecture

The OFM, which are obtained through the GA process, is given into the Conv_Layer1 of the existing LeNET architecture, which is designed with 32 Convolutional filters. The response size from this Conv_Layer1 is reduced by passing them into Pool_Layer1 (Max_Pool layer). The pooled sequences from Pool_Layer1 are given into the Conv_Layer2 of the existing LeNET architecture, designed with 64 Convolutional filters. The size of the response from this Conv_Layer2 is reduced by passing them into Pool_Layer2. The pooled sequences from Pool_Layer1 are given into three consecutive Dense layers, which produces the classified responses. The number of neurons in each Dense layer is set into 64. This existing LeNET architecture is modified into parallel LeNET architecture by changing the number of Conv_Layer and Pool_Layer in the form of parallel, as depicted in Fig. 5(b). The Conv_Layer1 and Conv_Layer 2 are designed with 64 Convolutional filters, and the dense layers in the conventional LeNET architecture are replaced by the FCM (Jiashun Chen et al. [23]). The FCM produces the classified results (either malicious node or non-malicious node). The entire workflow algorithm of the proposed method stated in this work is illustrated in Algorithm 1.

Input: Nodes;

Output: Classification response (malicious or non-malicious)

Start;

Step 1: Compute mutual information feature from the test sensor node.

Step 2: Compute redundancy metric feature from the test sensor node.

Step 3: Compute distance metric feature from the test sensor node.

Step 4: Integrate all the computed features, and they are called feature vectors.

Step 5: Optimize this feature vector using GA.

Step 6: The optimized feature vector from step 5 are classified using the proposed LeNET classifier (modified LeNET architecture), which produces the responses as either malicious or non-malicious.

End;

Algorithm 1 Malicious Sensor Node Classification

RESEARCH ARTICLE

4. RESULTS AND DISCUSSIONS

The proposed malicious sensor node classification system is simulated using the Network Simulator (NS2) tool with the hardware specifications of 2 GB RAM and Core i3 processor. The simulation environment of this proposed methodology consists of 100 sensor nodes, in which 20 sensor nodes are assumed to behave malicious behaviour, and the remaining sensor nodes are assumed to behave non-malicious behaviour. All the sensor nodes in WMSN initially have 1000 J of energy, and they are spread with 100 m width and 100 m length simulation environment.

The simulation environment is split into training and testing works. In this paper, the testing work contains more data than the training work to increase the classification accuracy of the proposed system. The training works trains 10 malicious sensor nodes and 20 non-malicious sensor nodes. The testing work tests or classifies 10 malicious sensor nodes and 60 non-malicious sensor nodes. The data rate or data transfer rate of each sensor node is fixed with 100 Mb/s. Table 1 shows the simulation parameters.

Table 1 Simulation Parameters

Parameters	Values
Total sensor nodes	100
Number of malicious sensor nodes	20
data rate	100 Mb/s
The energy level of each sensor	1000 J
Simulation area	100 m width and 100 m length

Figure 6 is the simulation environment of the proposed design in the NS2 simulation tool.

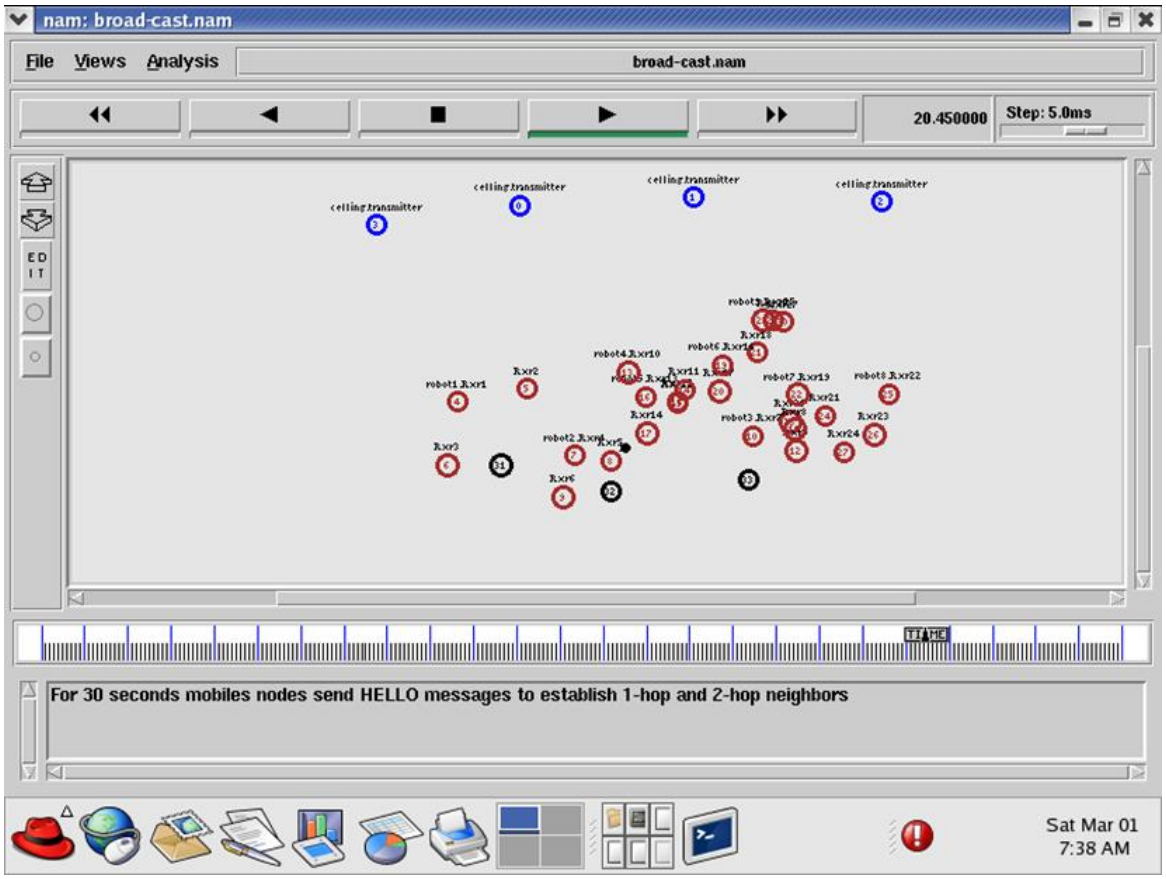

Figure 6 Simulation Environments in NS2

The following parameters are used to analyze the performance of the proposed malicious sensor node detection system. The Misclassification rate is determined in equation (13)

$$MisclassificationRate(MR) = \frac{FP+FN}{TP+TN+FP+FN} \quad (13)$$

Whereas TP is the total number of packets transferred correctly, TN is the total number of packets received correctly, FP is the total number of packets transferred incorrectly, and FN is the total number of packets received incorrectly.

RESEARCH ARTICLE

F1-score parameter is computed by equation (14)

$$F1 - Score = \frac{2*P*R}{P+R} \quad (14)$$

Whereas P is Precision and R is Recall, which is computed through the equations (15) and (16).

$$Precision(P) = \frac{TP}{TP+FP} \quad (15)$$

$$Recall(R) = \frac{TP}{TP+FN} \quad (16)$$

The accuracy and classification rate are computed through equations (17) and (18).

$$Accuracy(ACC) = \frac{TP+TN}{TP+TN+FP+FN} \quad (17)$$

$$ClassificationRate(CR) = \frac{Numberofmaliciousse\vee nodedetected}{Totalnumberofmalicioussensornodes} \quad (18)$$

Table 1 is the analysis of CR based on features. The proposed work with mutual information alone obtains 67% of CR, the proposed work with Redundancy metric alone obtains 71% of CR, the proposed work with Distance metric alone obtains 69% of CR, the proposed work with Mutual information+ Redundancy metric alone obtains 78% of CR, the proposed work with Mutual information+ Distance metric alone obtains 81% of CR, and the proposed work with Mutual information+ Redundancy metric+ Distance metric alone obtains 98% of CR.

Table 1 Analysis of CR Based on Features

Performance analysis parameters	CR (%)
Mutual information	67
Redundancy metric	71
Distance metric	69
Mutual information+ Redundancy metric	78
Mutual information+ Distance metric	81
Mutual information+ Redundancy metric+ Distance metric	98

Table 2 shows the simulation results of the proposed system. The proposed method achieves a 22% of misclassification rate, 89.5% of F1-score, 95.7% of precision, 95.6% of recall rate, 98.1% of accuracy and 98% of classification rate.

Table 3 is the malicious node detection time analysis using different deep learning architectures for detecting 10 numbers of malicious sensor nodes. The proposed LeNET architecture stated in this work consumed 0.6 ms of detection time, where the conventional LeNET architecture consumed 1.1 ms of detection time, AlexNet architecture consumed 1.8 ms of detection time, and Google Net architecture consumed 2.1 ms of detection time.

Table 2 Simulation Results of the Proposed System with Respect to Parallel LeNET and Conventional LeNET Architectures

	Simulation results (%)	
Performance analysis parameters	Parallel LeNET (modified LeNET)	Conventional LeNET (Alzubaidi et al. 2021)
Misclassification Rate	22	29
F1-Score	95.7	92.9
Precision	93.8	90.7
Recall	95.6	92.8
Accuracy	98.1	94.2
Classification Rate	98	94

Table 3 Malicious Node Detection Time Analysis using Different Deep Learning Architectures

Deep learning architecture	Detection time (ms)
Parallel LeNET (modified LeNET)	0.6
Conventional LeNET (Alzubaidi et al. 2021)[11]	1.1
AlexNet(Alzubaidi et al. 2021)[11]	1.8
Google Net(Alzubaidi et al. 2021)[11]	2.1

Table 4 shows the performance comparisons of the proposed method with conventional methods in WMSN. In this paper, the performance of the proposed algorithm is compared with other conventional algorithms.

Zhiming Zhang et al. [9] obtained 31% of MR, 93.6% of F1-score, 90.7% of precision, 93.2% of recall, 95.9% of accuracy and 96% of CR. Koyuncu et al. [12] obtained 43% of MR, 91.6% of F1-score, 89.7% of precision, 89.9% of recall, 92.8% of accuracy and 92.7% of CR. Ahmed Salim et al. [13] obtained 47% of MR, 92.1% of F1-score, 87.6% of precision, 81.7% of recall, 91.4% of accuracy and 91.8% of CR. Nidhya et al. [24] obtained 29% of MR, 93.9% of F1-score, 91.7% of precision, 92.6% of recall, 96.7% of accuracy and 95% of CR. Chen Jian et al. [25] obtained 39% of MR, 90.6% of F1-score, 86.5% of precision, 84.7% of recall, 90.7% of accuracy and 93.7% of CR.

RESEARCH ARTICLE

Table 4 Performance Comparisons of the Proposed Method with Conventional Methods in WMSN

Methodology	Simulation Results (%)					
	MR	F1-Score	Precision	Recall	Accuracy	CR
Proposed work	22	95.7	93.8	95.6	98.1	98
Zhiming Zhang et al. (2021)[9]	31	93.6	90.7	93.2	95.9	96
Nidhya et al. (2021)[24]	29	93.9	91.7	92.6	96.7	95
Koyuncu et al. (2019)[12]	43	91.6	89.7	89.9	92.8	92.7
Ahmed Salim et al. (2018)[13]	47	92.1	87.6	81.7	91.4	91.8
Chen Jian et al. (2013)[25]	39	90.6	86.5	84.7	90.7	93.7

5. CONCLUSIONS

The main problem of this high energy consumption is solved by detecting the malicious behaviour sensor nodes which transfer multimedia information like a scalar, audio and video in WMSN. The internal layers of the existing LeNET architecture are modified into parallel, and the dense layers in the existing LeNET architecture are replaced by Fuzzy C Means (FCM) algorithm. This improves the malicious node classification accuracy and reduces the malicious node detection time significantly when compared with the conventional LeNET architecture for the malicious node detection process. The detection of malicious behaviour sensor nodes among the set of sensor nodes is a complex task due to its similar characters with normal sensor nodes in multimedia networks. This paper proposes an efficient methodology for detecting and mitigating the malicious nodes using feature index, which is optimized by a Genetic Algorithm (GA). The modified LeNET classification approach classifies the optimized feature set. The proposed method achieves a 22% misclassification rate, 95.7% F1-score, 93.8% precision, 95.6% recall rate, 98.1% accuracy, and 98% classification rate. The main limitation of this paper is that this work is not analyzed concerning energy and power consumption.

REFERENCES

[1] Jin, S., Yuanzhi, W. & Yining, S., “Design and implementation of wireless multimedia sensor network node based on FPGA and binocular vision”, J Wireless Com Network (2018) 2018: 163.

[2] Zou K., Ouyang Y., Niu C., Zou Y. (2012) Simulation of Malicious Nodes Detection Based on Machine Learing for WSN. In: Liu C., Wang L., Yang A. (eds) Information Computing and Applications. ICICA 2012. Communications in Computer and Information Science, vol 307. Springer, Berlin, Heidelberg.

[3] Roman, R., Zhou, J., Lopez, J.: Applying intrusion detection systems to wireless sensor networks. In: CCNC 2006: Proceeding of the 3rd IEEE Consumer Communications and Networking Conference, pp. 640–644. IEEE, NJ (2006)

[4] Kaplantzis, S., Shilton, A., Mani, N., et al.: Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines. In: ISSNIP, vol. 10, pp. 335–340 (2007).

[5] Liu, H., Cui, J., Dai, H.: Malicious nodes detecting in wireless sensor networks based on multivariate classification algorithm. Journal of Sensor Technology 24, 771–777 (2011).

[6] Xiao, D., Chen, C., Chen, G.: Intrusion detection based security architecture for wireless sensor networks. In: ISCIT 2005: Proceeding of the International Symposium on Communications and Information Technologies, pp. 1365–1368. IEEE, WuHan (2005).

[7] Shaikh RA, Jameel H, d’Auriol BJ, Lee H, Lee S (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712.

[8] Huang X, Fang Y (2008) Multiconstrained qos multipath routing in wireless sensor networks. Wirel Netw 14(4):465–478.

[9] Zhiming Zhang, Yu Yang, Wei Yang, Fuying Wu, Ping Li, XiaoyongXiong, "Detection and Location of Malicious Nodes Based on Homomorphic Fingerprinting in Wireless Sensor Networks", Security and Communication Networks, vol. 2021, Article ID 9082570, 12 pages, 2021.

[10] L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry and S. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," in IEEE Access, vol. 9, pp. 128765-128785, 2021.

[11] Alzubaidi, L., Zhang, J., Humaidi, A.J. et al. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. J Big Data 8, 53 (2021).

[12] M. Koyuncu, A. Yazici, M. Civelek, A. Cosar and M. Sert, "Visual and Auditory Data Fusion for Energy-Efficient and Improved Object Recognition in Wireless Multimedia Sensor Networks," in IEEE Sensors Journal, vol. 19, no. 5, pp. 1839-1849, 1 March1, 2019.

[13] Ahmed Salim, WalidOsamy and Ahmed M. Khedr , “Effective Scheduling Strategy in Wireless Multimedia Sensor Networks for Critical Surveillance Applications”, Appl. Math. Inf. Sci. 12, No. 1, 101-111 (2018).

[14] Harsh Bhatt; MalaramKumhar, “QoE Aware Routing Protocols in Wireless Multimedia Sensor Networks: A Survey”, IJCSN - International Journal of Computer Science and Network, Volume 7, Issue 1, February 2018.

[15] J. Pournazari, M. Alaei and F. Yazdanpanah, "A method for coverage optimization in wireless multimedia sensor networks," 2016 Eighth International Conference on Information and Knowledge Technology (IKT), Hamedan, 2016, pp. 128-133.

[16] Li W. (2012) PSO Based Wireless Sensor Networks Coverage Optimization on DEMs. In: Huang DS.,Gan Y., Gupta P., Gromiha M.M. (eds) Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence. ICIC 2011.

RESEARCH ARTICLE

Lecture Notes in Computer Science, vol 6839. Springer, Berlin, Heidelberg.
[17] Domínguez-Medina C., Cruz-Cortés N. (2010) Routing Algorithms for Wireless Sensor Networks Using Ant Colony Optimization. In: Sidorov G., Hernández Aguirre A., Reyes García C.A. (eds) Advances in Soft Computing. MICAI 2010. Lecture Notes in Computer Science, vol 6438. Springer, Berlin, Heidelberg.
[18] Zhao Jing, Zeng Jian-Chao, "A virtual centripetal force-based coverage-enhancing algorithm for wireless multimedia sensor networks", Sensors Journal (IEEE), vol. 10, no. 8, pp. 1328-1334, 2010.
[19] Haining Chen, Hongyi Wu, Nian-Feng Tzeng, "Grid-based Approach for Working Node Selection in Wireless Sensor Networks", Communications IEEE International Conference, vol. 6, pp. 3673-3678, 2009.
[20] Muhammad Kamal Amjad, ShahidIkramullah Butt, RubeenaKousar, et al., "Recent Research Trends in Genetic Algorithm Based Flexible Job Shop Scheduling Problems," Mathematical Problems in Engineering, vol. 2018, Article ID 9270802, 32 pages, 2018.
[21] Li X, Zhang J, Yin M., "Animal migration optimization: an optimization algorithm inspired by animal migration behavior," Neural Comput & Applic., vol. 24, no. (7–8), pp. 1867–1877, 2013.
[22] Rinki Gupta, SreeramanRajan, "Comparative Analysis of Convolution Neural Network Models for Continuous Indian Sign Language Classification", Procedia Computer Science 171 (2020) 1542–1550.
[23] Jiashun Chen, Hao Zhang, Dechang Pi, Mehmed Kantardzic, Qi Yin, Xin Liu, "A Weight Possibilistic Fuzzy C-Means Clustering Algorithm", Scientific Programming, vol. 2021, Article ID 9965813, 10 pages, 2021.
[24] M. S. Nidhya, Dr. M. Vanitha, Dr. L. Jayanthi, Mr. L. Vadivel Kannan, Mr. S. Ajay, Mr. S. Gowdham Kumar, Dr. S. Sangeetha. (2021). A Detection of Malicious Nodes in HCCT Model for Wireless Sensor Network. Annals of the Romanian Society for Cell Biology, 1570–1579.
[25] Chen Jian, Zhang Lu, KuoYonghong, "Coverage-enhancing algorithm based on overlap-sense ratio in wireless multimedia sensor networks", Sensors Journal (IEEE), vol. 13, no. 6, pp. 2077-2083, 2013.

Authors

S. Arockia Jayadhas graduated in Electronics & Telecommunication Engineering at Sathyabama University, Chennai in 2008. He secured Master of Engineering in Applied Electronics at Sathyabama University, Chennai in 2011. He is Pursuing Ph.D. in the field of Wireless Sensor Networks at Sathyabama Institute of Science and Technology, Chennai, India. He is in teaching profession for more than 12 years. He has presented number of papers in National and International Journals, Conference and Symposiums. His main area of interest includes Wireless sensor Networks and Internet of Things.

S. Emalda Roslin born on 7.8.1979, received her Bachelor's degree in Electronics and Communication Engineering from St. Josephs College of Engineering, Chennai in 2000. She received Master's degree in Applied Electronics from Sathyabama University, Chennai in 2004 and her Ph.D. in 2013 from Sathyabama University. She completed her doctoral research in "An Energy Efficient Topology Control Algorithm for Enhanced Network lifetime in Wireless Sensor Networks". She is currently working as a Professor in the Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai and she is having 19 years of teaching experience. She has published more than 50 research papers in various International/National Conferences and International / National Journals indexed in Web of Science/ Scopus/other databases. She is guiding around seven research scholars. Her major areas of interest are wireless multimedia networks, wireless mesh networks and image processing. She is also an editorial board member for various journals.

How to cite this article:

S. Arockia Jayadhas, S. Emalda Roslin, "Performance Analysis of Malicious Node Detection in Wireless Multimedia Sensor Networks using Modified LeNET Architecture", International Journal of Computer Networks and Applications (IJCNA), 9(2), PP: 179-188, 2022, DOI: 10.22247/ijcna/2022/212334.