Intrusion Detection for Vehicular Ad-Hoc Network Based on Deep Learning

Rasika Vitalkar, Samrat Thorat and Dinesh Rojatkar

October 30, 2023

Intrusion Detection for Vehicular Ad-hoc Network based on Deep Learning

[1] Rasika S. Vitalkar
Department of Electronics Engineering
Government College of Engineering,
Amravati, India
rasikavitalkar15@gmail.com

[2]Samrat S. Thorat
Department of Electronics Engineering
Government College of Engineering,
Amravati, India
samratthorat@gmail.com

[3]Dinesh V. Rojatkar
Department of Electronics Engineering
Government College of Engineering,
Amravati, India
dinesh.rojatkar@gmail.com

***Abstract*— The proposed model of Deep learning algorithm namely Deep Belief Network is used for detecting intrusion in the vehicular ad-hoc network (VANET). Deep belief network algorithm gives more accuracy for intrusion detection in the network than existing methodologies such as machine learning algorithms or another deep learning algorithm. Now day automation is more important in all fields, similarly automatic vehicles i.e. driverless cars. These types of vehicles will come to market and all these vehicles are connected through a wireless network. All the vehicles are communicating with each other by sending some informative packets but there is an attacker who accesses that data and changes the data which may affect the security of the vehicle and also damage the system responsible for the accident. So intrusion detection system for the vehicular ad-hoc network is important with maximum accuracy. For this purpose used the updated CICIDS2017 dataset for training, testing and evaluation process. Experimental results using a deep Belief network for intrusion detection mechanisms proved that the proposed model could have good results on multi-class and binary classification accuracy 90% and 98% respectively.**

***Keywords*— Wireless Network, Cluster Head, Intrusion Detection System, Vehicular Ad-hoc Network, Deep Learning.**

I. INTRODUCTION

The Vehicular Ad-hoc Network is one of the types of Mobile Adhoc Network (MANET), because the communication node is a vehicle and an important part of intelligent transportation systems [1]. There are two types of communication systems for exchanging information between nodes in VANET. One is vehicle-to-vehicle and the other is vehicle-to-infrastructure [2]-[3]. Deployed by interconnected vehicles and infrastructure, VANET extends the security vulnerabilities derived from wireless communication system, especially in Distributed DOS attacks [4]. Variety of services has been designed for VANET, which are classified into two categories: commercial and security services. Most of them depend on a variety of collected data or transmitted to vehicular nodes. Making the VANET network more secure has become a major challenge as it has become easier for attackers to manage vehicles.

Extensive research is underway to secure network systems and to control the intrusions. Hoppe et al [5] An Intrusion Detection System (IDS) was proposed in the vehicle. Significant attack patterns such as increasing message numbers and missing message IDs can be identified. Larsen et al. [6] proposed feature-based techniques for detecting IDS attacks. This proposed technique compared the behavior of the current specification system with pre-defined patterns. Kamran Zaidi et. al. [7] proposed the intrusion detection system based on detecting false information using statistical analysis on VANET. Using this approach reduces the network message congestion. H. Sedjelmaci et. al. [8] suggested the mechanism for intrusion detection called as ELIDV for VANET. In this approach designed various set of rules for malicious vehicle detection. David A. Schmidt et. al. [9] suggested the mathematical model for intrusion detection based on spline function. Fuad A. Ghaleb et. al. [10] proposed the misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning technique on NSL-KDD dataset. The random forest algorithm is used as classifier, to aggregate the data by voting scheme. This mechanism is very effective for reducing the communication overhead. Khattab M. Ali Alheeti et. al. [11] suggested the mechanism for intrusion detection on VANET. Their mechanism extracts the minimum feature from trace file and analyzes the normal or abnormal behavior of vehicle. The artificial neural network and fuzzy logic were used to detect the attack.

Therefore, our aim to propose a strong and competent security mechanism to protect such networks against intruders, such as the use of network traffic monitoring and management services. This article proposed a deep learning approach to identify intrusions by studying recent research. Deep learning has been studied extensively in machine learning research, including signal processing, image processing, speech recognition, and more and widely used for practical applications. Once the system features are trained, the proposed system monitors the exchange packets in the network of vehicles to decide whether the system is being attacked. Since DNN takes less time to make a decision, the system responds quickly to an attack.

II. PROPOSED METHODOLOGY

A. Data Set

This research used the CICIDS2017 dataset available from https://www.unb.ca/cic/datasets/ids-2017.html which is related to the real world. According to Iman Sharafaldin et al.[12] The CICIDS 2017 dataset contains eight different five-day files and traffic data of the Canadian Institute of Cyber Security. Only 83 statistical features are extracted from the total dataset for network traffic. All the packets in the network flow from source to destination or destination to source.

B. Pre-Processing

All machine learning algorithms are correlated with the data in the dataset, and to get accurate results, this data must be preprocessed or cleaned. It normalizes all the values from the dataset and removes the features which have zero values in the dataset and are not required to train or test the system. First, we identify rows in a dataset that has lost values, infinite values , and meaningless values. This step is important to maintain the reliability of the dataset and avoid noise, so choosing the method has to be done carefully. Finally, checked and removed all duplicate rows. As a result of cleaning and feature removal methods, we end up with 2414417 examples and a dataset of 79 features.

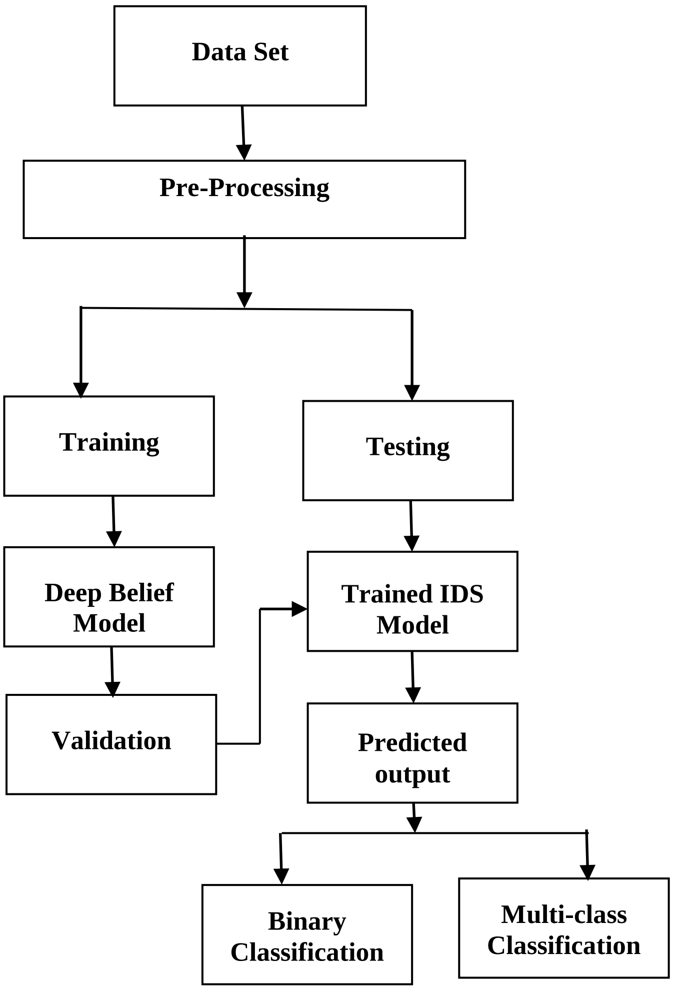

Fig. 1. Block Diagram for Proposed System

C. Deep Belief Network Model

For these proposed works deep belief network algorithm of deep learning is used to train the system with some tuning parameter. It creates some hidden layers and visible layers to train the system. The model has three layers; Input, hidden, and output. Each layer has assigned various neurons with weight. Select the hidden layer with its parameter using the selective method for processing. After the processing data is transformed from the next layer for further processing. The mathematical defined as

$$A = N^p \times N^q \tag{1}$$

Where, p is the input $m = m_1, m_2, m_3, \ldots \ldots . m_p$
q is the output of A(m), The Numerical representation of each layer is defined as

$$h_i(m) = f(w_i^T m + c_i) \tag{2}$$

Where, $h_i: N^{d_i - 1} \rightarrow N^{d_i}$

$$f: N \rightarrow N, w_i \epsilon N^{d \times d_i - 1}, b \in R^{di} \tag{3}$$

d_i *represent the size of input*

f is the nonlinear function which has sigmoid value (0,1)

In a classification of multiclass, our DBN model used the softmax function as a nonlinear function. The Softmax function expects the probability of each class and selects the largest of the probability values to give a more accurate value.
Mathematical representation of Sigmoid, Softmax, and Tangent function is as follows

$$Sigmoid = \frac{1}{1 + e^{-x}} \tag{4}$$

$$Tangent = \frac{e^{2x} - 1}{e^{2x} + 1} \tag{5}$$

$$Softmax = \frac{e^{mi}}{\sum_{j=1}^{m} e^{mi}} \tag{6}$$

For many hidden layer, DBN is defined as

$$H(m) = H_i(H_{i-1}\left(H_{i-2}\left(\ldots . . (H_i(m))\right)\right)) \tag{7}$$

This way of stacking hidden layers is typically called deep Belief networks. The DBN model has a more advanced feature with each hidden layer with a strong activation function like ReLU. The ReLU has good capability as compared to other nonlinear functions for trained the model [13]. The hidden layer has several layers with maximum neurons represent the width of DBN.

D. Loss Function

In the proposed model, includes loss function by finding optimal parameters for better performance. The loss function is used to measure the difference between predicted and target values [14]. The mathematical representation can be defined as follows

$$d(t1, p1) = |t1 - p1| \tag{8}$$

Where $t1$represent the targeted value

$p1$ represent the predicted value

For multiclass classification used negative probability with $t1$ as targeted value class and $p1(pad)$ probability as follows

$$d(t1, p1(pd)) = -\log\left(p(pd)\right) t \tag{9}$$

Model received the various input and output for training So decrease the loss mean is defined as follows

$$Loss(Input, output) = \frac{1}{m} \sum_{i=1}^{m} d\left(d(t1, p1), h_i(m)\right) \tag{10}$$

E. Validation

After trained the model validation is required to check whether the training for the model using a deep belief network is accurate or not. For both binary and multiclass classification validation result is given by confusion matrix. Before training, we have to select the classification type

F. Trained Intrusion Detection System Model

If the validation result is proper then save that model for testing and then test data is tested using that save intrusion detection model which gives the output.

G. Predicted Output

The output is in two forms binary and multiclass if we select binary then it shows output the data is malicious or normal and for multiclass classification it shows the output as the name of attack such as Denial of Service Attack (DoS), Distributed Denial of Service Attack (DDoS), PortScan Attack, Patator Attack, Web Attack, Botnet, Normal, etc.

III. Results & Discussion

The simulation and performance of proposed model can designed in MATLAB software with necessary system configuration MS Win-10 OS, Intel Core i3 CPU, 8-GB RAM, 2-GB Graphic cards etc.

A. Confusion Matrix

Fig. 2. Validation Confusion Matrix for Binary Classification

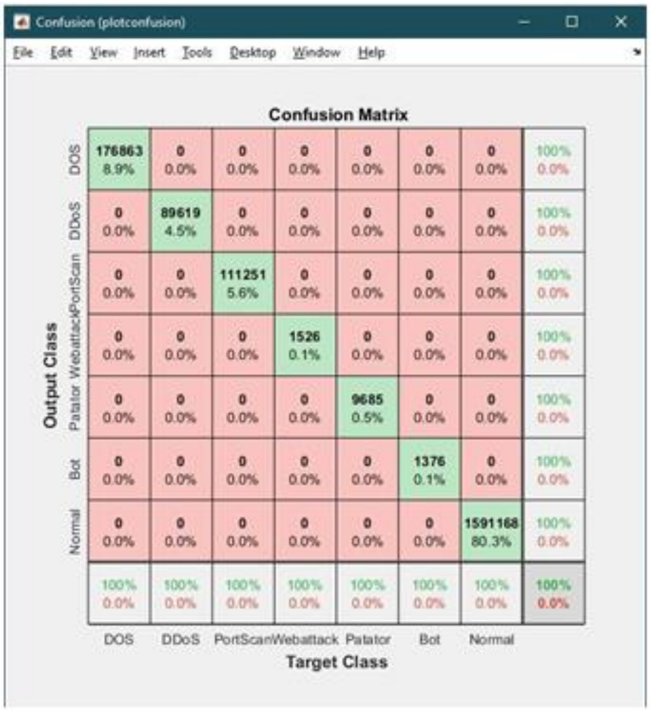

Fig. 3 Validation Confusion Matrix for Multiclass Classification

Confusion Matrix for both Binary Classification and for Multiclass Classification gives 100% accuracy it states that training for both classification is accurate and proper.

Number of live nodes at 600 seconds, 700 seconds and 800 seconds

B. Confusion Matrix Result

To show the performance of proposed methodology confusion matrix is used. A confusion matrix is a table that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known. Each row in a confusion matrix represents an actual class, while each column represents a predicted class. The confusion matrix gives you a lot of information, such as accuracy, precision, sensitivity, specificity etc.

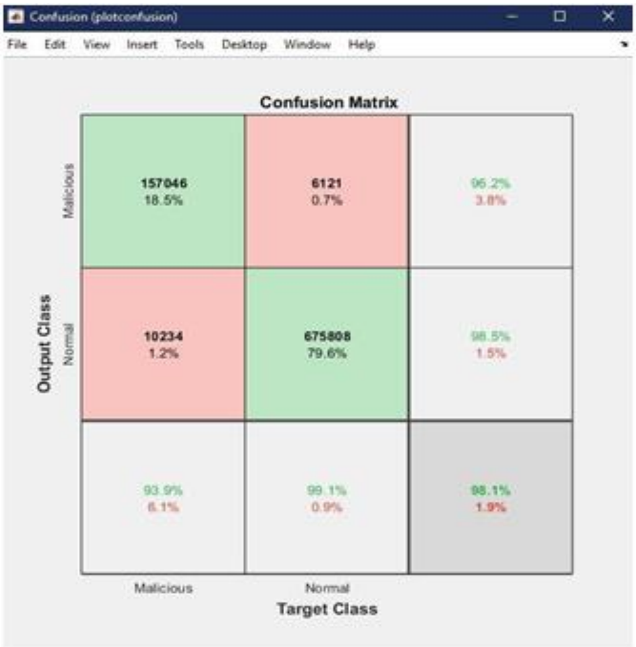

Fig. 4. Confusion Matrix for Binary Classification

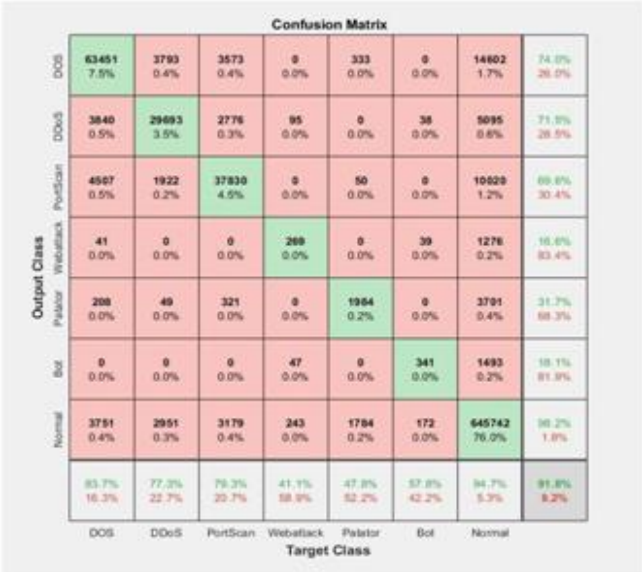

Fig. 5. Confusion Matrix for Multiclass Classification

C. Binary Classification Result

From the confusion matrix we get true positive (TP), False Positive (FP), True Negative (TN), False Negative (FP) for binary classification. From these all values we calculate the parameters value such as Accuracy, Specificity, Sensitivity, etc which all given in following table.

TABLE I. PARAMETERS VALUE FOR BINARY CLASSIFICATION

Parameters	Values
True Positive	10234
True Negative	6121
Accuracy	1.9259
Sensitivity	99.1024
F-Score	96.2486
Negative Predictive Rate	6.1179
False Positive Rate	80.786

Rate of Positive Prediction	93.8665
True Positive	10234
True Negative	6121
Accuracy	1.9259
Sensitivity	99.1024

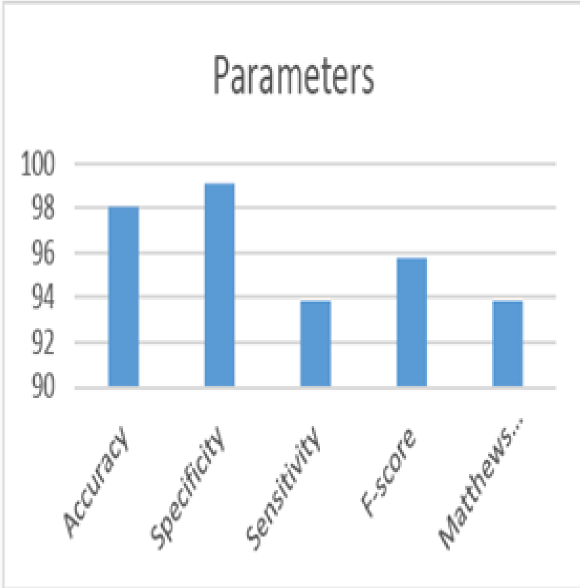

Fig. 6. Predicted Result for Binary Classification

D. Multiclass Classification Result

From confusion matrix for multiclass classification we get all parameter values for each attack type so the accuracy, specificity, sensitivity, f score are different for all attacks i.e. for DoS attack, DDoS attack, Web Attack, etc.

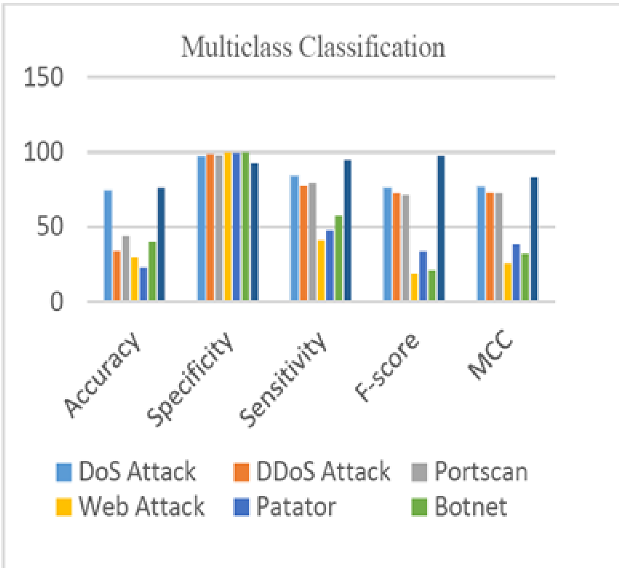

Fig. 7. Predicted result for Multi-class Classification

TABLE II. PARAMETERS VALUE FOR MULTICLASS CLASSIFICATION

Parameter	DoS	DDoS	Portscan	Web Attack	Patator	Bot	Normal
True Positive	63451	29693	37830	269	1984	341	645742
False Negative	12347	8715	9849	385	2167	249	36187
True Negative	75110	798957	785031	847199	840779	847079	155200
False Positive	22301	11844	16499	1356	4279	1540	12080
Accuracy	7.47178	3.49655	4.45473	0.031676	0.233629	0.040155	76.0404
Error Rate	2.6261	1.3947	1.9429	0.15968	0.050388	0.18135	1.4225
Sensitivity	83.7107	77.3094	79.3431	41.31315	47.7957	57.7966	94.6934
Specificity	97.1166	98.5392	97.9416	99.8402	99.4936	99.8185	92.7786
F-Score	75.7523	72.5791	71.3787	18.8007	33.9691	21.0131	97.4494
Positive Predictive Rate	73.9936	71.4857	69.6313	16.5538	31.6781	18.1287	98.1636
Negative Predictive Rate	98.3828	98.921	98.7209	99.9546	99	99.9706	81.0922
False Negative Rate	16.2893	22.6906	20.6569	58.8685	52.2043	42.2034	5.30656
False Positive Rate	2.8835	1.4608	2.0584	0.1598	0.50636	0.18147	7.2214
Rate of Negative Predictions	89.9021	95.1087	93.6024	99.8086	99.2625	99.7785	22.5371
Rate of Positive Prediction	10.0979	4.89126	6.3976	0.191355	0.73751	0.2215	77.4629
Matthews Correlation Coefficient	76.4851	73.077	72.7026	26.0073	38.5471	32.2923	83.2627

CONCLUSION AND FUTURE SCOPE

From this complete work conclude that deep belief network gives better accuracy or parameter values than the existing methodologies. For binary classification it gives good accuracy but for multiclass classification accuracy is low because of the availability of data for particular attack is low it may improve if same number of data will available or real world data will available. The future scope of these work is that use the Vehicular ad-hoc network dataset which having normal and malicious data for automatic vehicles which gives proper result.

REFERENCES

[1] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," in IEEE Access, vol. 7, pp. 154560-154571, 2019, doi: 10.1109/ACCESS.2019.2948382.

[2] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, “Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions,” IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1314–1345, Second quarter 2019.

[3] X. Hu, J. Zhao, B. Seet, V. C. M. Leung, T. H. S. Chu, and H. Chan, “Saframe: Agent-based multilayer framework with context-aware semantic service for vehicular social networks,” IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, pp. 44–63, March 2015.

[4] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: Future challenges,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898–2915, Nov 2017.

[5] T. Hoppe, S. Kiltz, and J. Dittmann, “Security threats to automotive can networks practical examples and selected short-term countermeasures,” Reliability Engineering and System Safety, vol. 96, no. 1, pp. 11-25, 2011.

[6] [6] U. E. Larson, D. K. Nilsson, and E. Jonsson, “An approach to specification-based attack detection for in-vehicle networks,” in IEEE Intelligent Vehicles Symposium, Proceedings, 2008.

[7] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," in IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6703-6714, Aug. 2016, doi: 10.1109/TVT.2015.2480244.

[8] H. Sedjelmaci and S. M. Senouci, "A new Intrusion Detection Framework for Vehicular Networks," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 2014, pp. 538-543, doi: 10.1109/ICC.2014.6883374.

[9] D. A. Schmidt, M. S. Khan and B. T. Bennett, "Spline Based Intrusion Detection in Vehicular Ad Hoc Networks (VANET)," 2019 Southeast Con, Huntsville, AL, USA, 2019, pp. 1-5, doi: 10.1109/SoutheastCon42311.2019.9020367.

[10] Fuad A. Ghaleb, Faisal Saeed, Mohammad Al-Sarem, Bander Ali Saleh Al-rimy, Wadii Boulila, A. E. M. Eljialy, Khalid Aloufi and Mamoun Alazab, "Misbehavior-Aware On-Demand Collaborative Intrusion Detection System Using Distributed Ensemble Learning for VANET", Electronics 2020, 9, 1411; doi:10.3390/electronics9091411

[11] K. M. Ali Alheeti, A. Gruebler and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2015, pp. 916-921, doi: 10.1109/CCNC.2015.7158098.

[12] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Purtogal, January 2018.

[13] P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou and D. Tzovaras, "An Intrusion Detection System for Multi-class Classification Based on Deep Neural Networks," 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), Boca Raton, FL, USA, 2019, pp. 1253-1258, doi: 10.1109/ICMLA.2019.00206.

[14] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334.P. Soreanu and Z. Volkovich, "Energy-Efficient Circular Sector Sensing Coverage Model for Wireless Sensor Networks," 2009 Third International Conference on Sensor Technologies and Applications, Athens, Glyfada, 2009, pp. 229-233, doi: 10.1109/SENSORCOMM.2009.45