IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

Jamming Attack Detection using Machine Learning Algorithms in Wireless Network

Aiswarya K and Dr.Vijitha S
Department of Electronics and Communication Engineering
NSS College of Engineering, Palakkad, Kerala, India

Abstract: *Due to technological improvements, a tremendous amount of data is generated every second. In the world of computing, data is being gathered constantly, from mouse clicks. In the system network, secure lines and servers must will be monitored. Such system were known as Intruder Detection System(IDS). A wireless network is the main target of such attacks, which result an undesirable denial of service. Fuzzy logic, game theory, channel surfing, and time series are several jamming detection methods that have been suggested over the past ten years. The majority of these methods are ineffective in locating intelligent jammers. Thus, effective, high-accurate and quick jamming detection approaches are highly required. For the purpose of detecting jamming attacks, a detailed analysis of certain ML algorithms including Random Forest, SVM, and NN, was performed and evaluate how well several machine learning algorithms detect jamming signals. In order to identify jamming signals, we looked into various signal characteristic types and produce a significant dataset and it will trained, analyzed, and tested using this dataset. The probability of detection, the probability of false alarm, the chance of miss detection, and accuracy were used to study and evaluate the performance of various algorithms. The simulation findings indicate that the random forest method used for jamming detection can identify jammers with high accuracy and detection probability, and low false alarm probability.*

Keywords: Jamming Attacks; Machine Learning; Random Forest; Neural Network; Support Vector Machine.

I. INTRODUCTION

Through broadcasting, the communication channels are flooded with radio signals in an aim to interfere with authorized users' communication by decreasing their SNR, jammers produce an undesirable denial of service. Using inexpensive and widely available software defined radio units like the universal software defined radio peripherals and the GNU radio, the attacks can be launched with ease. There are four basic categories of attacks by jammers: reactive, deceptive, random, and constant jammers. Attacks are carried by persistent jammers by sending out a noise which is continuous and have high-power that sweeps from one channel to another while employing a predetermined approach, repeatedly doing so over time. Random Jammers that creates most serious security threats in the field of WSNs and sleeps for a random of time and creates interruption in transmission. To keep wireless channels busy, deceptive jammers transmit erroneous packets via them. Reactive jammers only focused on the frequency channels that are used for communication while continuously monitoring the situation of the other channels. Jammers can also be divided into two categories: regular and smart. Regular jammers all play at once since they are unable to detect the current transmitted signals. Smart jammers can update their assault techniques or change the transmission power to severely disrupt valid transmissions. They can also catch information quickly, sense signals, and determine how the users emits their signals.

There have been several potential jamming detection methods. The two categories are machine learning-based and non-machine learning-based. Fuzzy logic, game theory, channel surfing, etc. are some of the techniques used by non-machine learning methods. However, they were ineffective in finding such intrusions. In the case of machine learning techniques, the first model calculates the throughput while the second model, based on the strength of the signal received to the channel, computes the unauthorised packet delivery ratio. By utilising these two parameters they were able to determine whether the link is being exploited or not.

In this work, we suggest using machine learning algorithms to determine whether a transmitter's and a receiver's transmission link is under attack. If the following processes are thoroughly used,ML based models can achieve

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

detection accuracy in high level: choosing the right features as input data, measuring, extracting, generating a substantial dataset, and implementing accurate methodology to evaluate the model. The following parameters are used to identify intruder attack by assessment of the following parameters: threshold, delay, throughput, packet arrival ratio, signal strength, and channel assessment. Also examined methods for determining the proper feature selection and communication link status. To evaluate machine learning models, we created a large dataset. To prevent the issue of underfitting, cross validation techniques and randomization, and normalisation of the dataset were used.

II. RELATED WORKS

In this literature, several methods proposed for detecting different kinds of intruder attacks / jamming attacks using different algorithms were explained in detail. The main aim of most of the techniques where finding the most accurate one among them.

Lama Alsulaiman and Saad Al-Ahmadi [1], stated that the WSN is a favoured option for numerous applications in a variety of industries, including healthcare, telecommunications, and even the detection of earthquakes, volcanoes, and flooding during natural calamities. WSN raises numerous security risks as a result of its extensive use. Due to a number of limitations, including limited processing power, battery life, and storage space, the WSN is susceptible to several types of assaults. The most common assault that can harm WSN is a DoS attack. By flooding the network with a large number of spurious requests, DoS attacks can damage a network service by preventing legitimate traffic from connecting to the network. To make sure the WSN is secure, the intrusion detection system (IDS) should be deployed. One of the popular approaches for enhancing IDSs' capacity to recognise and identify attackers is the use of ML techniques. For detecting Denial of Service attack in WSN, ML algorithms has been applied. In order to determine, among the model which one categorises the data set the best, this study investigates many classification models, such as Naive Bayes, NN, SVM, and Random forest. In order to compare effectiveness of techniques in identifying DoS attacks, various comparison metrics, including recall, accuracy, and precision, are used. They are also tested on the WSNDS dataset, a specialised WSN dataset that contains both typical attack scenarios and multiple attack scenarios.

Mohammed Alsahli, Almasri, Mousa, Abdulaziz, Alwairadhi [2], suggested that new security threats and concerns emerge as a result of the quick development of technology, creating a hot topic for research. The Wireless Sensor Network (WSN) is made up of dispersed wireless sensor nodes that collect unfiltered environmental data. Each Sensor node has a small micro-controller, a power source, and a radio transceiver. These nodes are tiny and only have a small amount of processing power. They are made with cheap cost and energy consumption in consideration, and as a result, have limited processing capacity and connectivity. There are number of possible security threats that could arise resulting from the sensors' limitations in memory, processing capability, and energy consumption. Protecting the WSN without access lot of processing power or energy is the main challenge. Due to the senor's limited computing power, it is challenging to incorporate traditional security methods like encryption. It is challenging to defend networks and applications against these assaults manually or using commonly available off-The Shelf technologies like firewalls, antivirus, IDS or IPS. This makes machine learning (ML) and artificial intelligence (AI) algorithms popular and ultimately necessary in such situations. WSN can be protected using AI in general and ML in particular by recognising and categorising potential assaults using previously discovered attack patterns.

Youness Arjoune,Fatima , Naima, Salahdine, Ghiribi[3], proposed that wireless network is the target of jammer attacks, which produce an undesirable denial of service. Despite the robustness provided by the utilisation of millimetre wave bands, 5G is susceptible to these attacks. Fuzzy logic, game theory,etc. are just a few of the jamming detection methods that have been suggested over the past ten years. The majority of these methods are ineffective in finding intelligent jammers. Therefore, there is a huge need for accurate and quick jamming detection methods.In this study, we evaluate how well several machine learning algorithms detect jamming signals. We examined several signal aspects that can be used to recognise jamming signals, and we used these factors to produce a large dataset. The ML algorithms were trained, tested, and evaluated using this dataset. These methods include NN,SVM and random forest. The probability of detection, and false alarm rate, the chance of false detection, and accuracy were used to study and evaluate the performance of various algorithms. The evaluation findings demonstrate that the random forest method used for jamming detection can identify jammers with high accuracy and low false alarm rate.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

Jani,Arto Juhola, Shahriar, Aarne,Ijaz [4], The fifth generation (5G) of mobile networks will face various issues that have been investigated by using machine learning (ML). ML will expose the network to a number of significant cyber security flaws, nevertheless. In machine learning, collected data is used to generate the majority of learning. Un-reviewed data will have adverse effects on the computers that use it to create network-actionable intelligence. On the other hand, scrutinising the data presents privacy issues. The majority of ML systems, unfortunately lifted from other fields that perform in tiny, closed situations. When these ML systems are used in 5G, the network may unintentionally become vulnerable to major security issues like unauthorised resource consumption, denial of service attacks, and the leakage of sensitive data.

Therefore, they examine the limitations of the most well-known ML systems that are actively being explored for implementation in 5G in this paper. They further categorise and investigate remedies for avoiding those issues in 5G networks.

Y.Wu,A. Khisti,Xiao, Caire,Wong, Gao [5], contributes that during recent years have seen a substantial increase in research interest in physical layer security, protects data secrecy based on information-theoretic techniques. The main concept underlying physical layer security is to make use of the transmission channel's inherent randomness to ensure physical layer security. Physical layer security research faces significant difficulties as we go toward 5G wireless communications. The physical layer security research on a variety of interesting 5G technologies, such as full duplex technology, enormous MIMO, millimetre wave communications, networks, and non-orthogonal multiple access, is surveyed in this study. The technical issues that are still being worked on at the time of writing are listed, and 5G and beyond physical layer security trends are examined.

J.Heo, J.Kim, J.Paek, S.Bahk [6], studied that jamming in wireless sensor networks has developed to be more energy-efficient,encrypted, and long-lasting. Attackers that want to remain undetected provide brief jamming signals, which consume less energy but are still potent enough to disrupt entire packet transport processes. Three different stealthy assault types—reactive jamming, jamming ACK, and fake ACK—are covered in this article. These assaults are harmful to low power and LLN applications because they disrupt communication and quickly deplete the batteries of LLN devices. We introduce Dodge-Jam, a simple anti-jamming method appropriate for LLN contexts, to resist these attacks. Dodge-Jam addresses hidden jamming attacks. By switching the acknowledgement exchange channel to a channel determined by the data packet, it secures the ACK packet. In addition, it aids the receiver in recovering the original packet from many incorrect packets received by splitting a data packet into multiple blocks and executing logical shifts of the blocks when retransmitting the packet. We put Dodge-Jam into use on real embedded devices and assess its effectiveness on a multi-hop testbed using mathematical analysis and tests.

GS.Kasturi , Ansh Jain , Jagdeep Singh[7],studied One such form of attack that interferes with genuine wireless signals by lowering the signal-to-noise ratio is known as Radio Frequency Jamming (RF-Jamming) attack. Many applications, especially those are safety-sensitive like self-driving cars, and are seriously at risk from these kinds of attacks. Therefore, it is essential to set up defences against these assaults and a trustworthy communication mechanism. Additionally, it's critical to understand the type of jamming assault that a network has been subjected, in order to take the proper precautions for defence against such attacks. In other words, it's important to classify these attacks in addition to detecting them. As a result, they address this issue in this study and suggest a machine learning-based categorization method for various jamming assault types. Using the network simulator ns-3,they simulate the jamming scenario in wireless ad-hoc networks and use the data obtained from the simulation to train and assess several algorithms. We assess the accuracy of each algorithm and present the findings, which reveal that the Gradient Boosting Algorithm can classify jamming assaults with an extremely high degree of accuracy.

Fang,Qian, Rose, Qingyang [8], showed how 5G mobile wireless network technologies' sophisticated characteristics to create new security requirements and issues. Comparing the security of wireless network to that of conventional cellular networks, this paper gives a thorough research. The article begins with a discussion of the unique characteristics of 5G networks, as well as the updated specifications and requirements for 5G security. By the consideration of new service requirements and new use cases in 5G networks, the potential attacks and security services are highlighted. Based on the corresponding security services, such as authentication, availability, confidentiality, and privacy etc. were the most recent developments and also current 5G wireless security methods are described. The novel security aspects involving many technologies used in 5G, such as heterogeneous networks, direct communications,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

massive multiple-input multiple-output (MMIMO), software-defined networks, and the IoT, are also examined in this study.They suggest a new 5G security architecture in response to these security research and development initiatives, on which the analysis to identity management and authentication is offered. To demonstrate the benefits of the suggested security architecture, we examine a handover process and a signalling load scheme as case studies. Finally, a summary of the difficulties and potential paths for 5G wireless security is provided.

O. Pu˜nal, I. Aktas¸, C. J. Schnelke, G. Abidin, K. Wehrle, and J. Gross[9], suggested that to detect jamming assaults, machine learning techniques should be based on algorithms such NN and SVM with different attributes. For instance, the authors suggested an approach based on artificial NN for wide band spectrum detection and cyclic spectral analysis. The algorithm separates jamming signals from narrow band transmissions based on signal quality and modulation.

K. Grover; A. Lim; Q. Yang [10]described SVM, adaptive boosting, and expectation maximisation algorithms for designing a ML-based jamming detection system. Jamming attacks were discovered using noise, busy channel ratio, packet delivery ratio, and maximum sleep time.

N. Sufyan, N. Saqib, M. Zia [11], illustrated how most of the methods previously demands for greater resources and eventually just act as a stop gap.. Although they can recognise that the link is down, they frequently struggle to locate the cause of the service interruption. Additionally, the chances of false alarm using these procedures is rather significant. To train and verify the classification models, they require specific algorithms. Although they are two of the most crucial steps in building machine learning-based detection algorithms, feature selection and learning curves are frequently overlooked. Thus, there is a critical need for quick and effective detection methods that can more effectively identify jamming attacks.

H. Reyes, N. Kaabouch [12]describes two timing channel-based methods for jamming detection. The second model calculates throughput, while the first model calculates the bad packet arrival ratio based on the signal strength. They were able to determine if the link is being attacked or not based on these two factors. Based on the received signal intensity, packet arrival ratio, bad packet ratio, and channel clear evaluation characteristics, the author of [16] suggested a fuzzy logic centralised jamming detection system. The detection method for this model was also created as a base station, to calculate the attack's duration. it computes the packet received ratio and the SNR ratio from the arrived data.

In [13], Almomani et al. generated a dataset with several DoS attacks, including blackhole, grayhole, flooding, and scheduling. The WSN-DS dataset was gathered with the goal of assisting experts in identifying DoS assaults in WSNs. This dataset was used by Almomani et al. to train an artificial NN (ANN) to recognise and categorise different types of DoS attacks. The simulation findings demonstrate that various DoS attack types could be identified more precisely. One hidden layer produced the greatest results.

M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan [14] gave a review of ML tools for identifying denial-of-service attacks. At each level of the TCP/IP protocol stack, the DoS variations were examined with an emphasis on network layer attacks.

S. Gunduz, B. Arslan, and M. Demirci[15], presented an analysis of the NSL-KDD dataset's performance in evaluating ML algorithms for intrusion detection in WSNs. However, just the capacity to identify intrusions was evaluated.

C. Ioannou, V. Vassiliou, and C. Sergiou in [16], employed ML methods to enhance WSN anomaly detection. A PhysioNet medical dataset was utilised in the experiment. The outcomes shows that the KNN algorithm was better for regression tasks while the J48 method outperformed in classification tests.

G. Pachauri and S. Sharma in [17], provided a simple detection technique utilising logistic regression that evaluated the behaviour of a lot of nodes while they were subjected to jamming and blackhole attacks. They took into account a number of variables, including attacker location, transmission power, and traffic volume. The authors also took into account several WSN topologies, including mesh multi-hop networks and central data collecting.

P. Nancy, S. Muthurajkumar, S. Ganapathy et. [18], explained a fuzzy temporal DT technique, a dynamic feature selection algorithm was put forth to choose the ideal number of features from a dataset. To accurately detect attacks, they enhanced the DT algorithm and combined it with NNs. The experiment shows the efficiency of the suggested method, employed the KDD Cup dataset.

P. Nancy, S. Muthurajkumar , presents danger theory which is rooted on the fundamental ideas of artificial immune technology, as a multi-stage IDS in [19], to safeguard WSNs. In order to produce output based on the weights and concentrations of parameters, the system continuously checks WSN parameters like as energy, data size, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

transmission frequency. The network's robustness is increased by nodes working together to detect intrusions; this results detection rates higher, less false alarm rates, and less energy consumption. However, as the number of nodes increases, the detection rate decreases and energy consumption rises.

R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman[20], utilised hybrid deep NNs (DNNs) to monitor network traffic and defend network from several blocks in a framework called Scale Hybrid IDS-AlertNet. Several datasets, including UNSW-NB15, Kyoto, WSN-DS,etc. were subjected to the DNN model. International Journal of Network Security Its Applications (IJNSA) out performes better by utilising conventional ML classifiers in terms of false alarm rate and detection accuracy. The issue with this strategy is that it necessitates a high computation power for integral part DNNs. Dept.

There are numerous detection models available. According to the literature review, machine learning jamming detection models may be employed successfully for intruder detection and can provide higher performance than conventional machine learning methods

III. JAMMING ATTACK DETECTION APPROACH BASED ON MACHINE LEARNING ALGORITHMS

From this study the detection of jamming attack evaluated as a classification problem where the classifier must decide between two states: either the link is lost due to jamming or the link is lost due to any other factor. The success of ML theory in handling complicated issues in an acceptable amount of time and with affordable resources is the motivation behind using this theory to solve such issue. The choice of appropriate features is essential for the design of an effective machine learning algorithm. To detect such kind of attacks in this work, a number of features were chosen.It is not enough to detect a intruders using just one parameter. Finding analytical relationships between these metrics and the link's status might also be challenging. These factors lead to the use of machine learning theory to identify an empirical relationship between these four indicators and the detection of jamming attacks. The four parameters used to identify jamming attacks, the feature selection process, and the jamming attack model are all covered in this section. Next section discuss the machine learning methods that were employed, including NN,SVM with linear kernel and random forests.

3.1 Jamming Attack Models

Attacks that jam wireless networks focus both physical layer and cross link-layer. In these attacks, those jamming signals keep the channel busy prevent the intended connection between a transmitter side A and a receiver side of location B. A denial of service may result from jamming signals that occupy at the channel for an enlarged length of time. Without the presence of jamming signal, the received signal at location B is given by, if the desired signal at location A is denoted by x(t) and the received signal at B is designated by:

$$y(t) = x(t) + n(t)$$

where x(t) is the desired signal , y(t) is the received signal, and n(t) between the transmitter and the receiver, there is additive white Gaussian noise. The jammers can create a signal called $x_j(t)$ to flood the channel by imitating the desired signals. The receive signal at position B is thus supplied as follows in the presence of the jammer signal:

$$y(t) = x(t) + x_j(t) + n(t) + n_1(t)$$

where $x_j(t)$ is the jammer signal and $n_1(t)$ is the noise within the path between the receiver and the jammer's location. As a result, the jamming detection issue can be formulated as a choice between two states, H_0 and H_a, for the receiver. When the received signal is not jammed, it is in the state H_0; when it is, it is in the state H_a. The ideal way to represent this challenge is as a classification problem where the machine learning classifier must categorize the received signal into class A, which denotes the intended transmission, or class B, which denotes a jamming signal.

3.2 Feature Selection

The metrics poor packet ratio, packet arrival ratio, received signal intensity, and clear channel evaluation are used to identify jamming attacks. The use of these four parameters is justified by the fact that all communication systems are fitted with network interface cards that have diagnostic features that enable the calculation of these metrics. One of the most crucial metrics for identifying jamming attempts is bad packet ratio. It speaks of the proportion of incomplete packages that were delivered. It is interpretable as and can be measured at the receiver end:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

PR=(Number of erroneous received packages / Total number received packages) The frame check sequence of the arriving packets is verified by the receivers at the mac level in order to calculate this bad packet ratio. When the connection state is good for transmission, the bad packet ratio is quite low, but it rises if the channel is good. The percentage of packages that are delivered correctly is known as the packet delivery ratio. At the transmitter end, it is measured and expressed as: PDR=(Number of packages delivered correctly / Total number of transmitted packages) Each time it gets a valid packet, the receiver sends a response packet to the transmitter. When the link is in good condition, the packet delivery ratio is very high, but if the link is being attacked, it loses value exponentially. The number of transmitter tries to send a package that are unsuccessful can be calculated using the clear channel evaluation. If jamming assaults are being used to block the channel, this parameter's value rises.

$$RSS = P_t G_t G_r h^2 * h^2/d^4$$

where P_t is the transmitter signal power, G_t and G_r is the antenna's gain at transmitter and receiver respectively, t and h_r are the height of antenna at transmitter and receiver, and d is the distance between transmitter and receiver. Equation is expressed as:

$$RSS = K(P_t/d^4)$$

where k is a constant such that

$$k = G_t G_r(h^2 h^2)$$

3.3 Machine Learning Algorithms

A. Random Forest

A hierarchical classifier technique called random forest consists of several decision trees. By sorting trees according to their feature values, the test data is classified using this method. One node and multiple branches comprise each decision tree. The test data feature that needs to be classified is represented by the decision node, and the branches are values that the node can forecast. To prevent the issue of overfitting, a high number of trees are used. The performance of the final model is improved as a result of the decreased system variance. The total number of trees to be created and factors relevant to decision trees, such as minimum split and it's criteria, can be basic random forest classifier parameters. A predictor called random forest gathers data from each tree. To train the forest, these trees are merged to get an aggregated estimation. Each tree may independently predict output values once the forest has been trained.

B. Support Vector Machine

To divide data into two classes, a support vector machine builds a hyperplane. The line separating the two classes is determined by the kernel selection. With this model, various kernels can be employed, including linear, cubic, radial, and quadratic kernels. One of the most well-liked supervised learning algorithms, SVM, or SVM, is used to solve Classification and Regression problems. However, it is largely employed in Machine Learning Classification issues. In order to accurately categorise new data points in the future, the SVM algorithm aims to determine the optimum line or decision boundary which can divides n-dimensional space into classes. A hyperplane is the name of this optimal decision boundary. SVM selects the extreme vectors and points that that contribute to the hyperplane's formation. Support vectors, which are used to represent these extreme instances, form the basis for the SVM method. Take a look at the diagram below, where two distinct categories are separated using a decision boundary or hyperplane.

- Linear SVM: The term "linearly separable data" refers to data that can be divided into two groups using only a single straight line. Linear SVM is used to classify such data.
- Non-linear SVM: When a dataset cannot be classified using a straight line, it is said to have been non-linearly separated.

C. Neural Network

A neural network is a programming paradigm with biological influences that allows a machine to learn from empirical data. This network has demonstrated a strong capacity for problem-solving and learning in a variety of research fields, including wireless communication, image processing, and signal processing. One input layer, one or more hidden layers, and an output layer make up a neural network. One or more neurons can be found in each layer. A neuron is made up of an activation mechanism and a number of linkages that link it to other neurons in various layers. Each link

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

has an initial weight, and during the learning phase the neural network looks for the set of ideal weights that minimises the error between the hypothesis function and the provided dataset labels. The forward propagation and reverse propagation ideas are the two essential components of each neural network. The simplest artificial neural network is forward propagation, which only allows information to pass through hidden layers from input to output. To reduce the cost function, neural networks employ a variety of optimization techniques, including Adam, gradient descent, and stochastic gradient descent.

IV. CONCLUSION

This paper examined various approaches for detecting jamming signals. By utilising the millimetre wave spectrum, wireless technology is intended to be resistant to intruder attacks. It is also intended to operate at wavelengths below 6 GHz, which jammers may easily target. To stop these attacks, clever jammer detection methods are needed. In this study, evaluated the jamming detection methods that are currently in use. We looked at and contrasted the effectiveness of various machine learning models to find jamming attacks. To train, validate, and test the random forest, SVM, and NN algorithms, feature extraction selection were carried out, and a sizable dataset was built. To assess the effectiveness of these models based on various criteria, we employed a cross-validation technique and supplied learning curves. The findings demonstrate that a random forest-based approach may identify jamming attempts very accurately and inexpensively.

REFERENCES

[1]. Lama Alsulaiman and Saad Al-Ahmadi(2021) , ”Performance evaluation of ML for DoS detection in WSN”, International Journal of Network Security Its Applications (IJNSA) Vol.13, No.2.

[2]. Mohammed S. Alsahli, Marwah M. Almasri, Mousa Al-Akhras and Abdulaziz I. AlIssa, Mohammed Alawairdhi(2021), “Evaluation of machine learning algorithms for intrusion detection system in WSN”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 5.

[3]. Youness Arjoune, Fatima Salahdine, Md. Shoriful Islam and Elias Ghribi,Naima Kaabouch(2020),”A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication,”IEEE Xplore,vol.9,pp.24-40.

[4]. Jani Suomalainen,Arto juhola and Shahriar Shahabuddin(2020),”Machine Learning Threatens 5G Security,” IEEE Access,vol.8, pp.128-142.

[5]. G.S Kasturi,Ansh Jain and Jagdeep Singh(2020),”Detection and Classification of Radio Frequency Jamming Attacks using Machine Learning,”div of inf. Technology, vol.8.pp.442.

[6]. Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao(2018), “A survey of physical layer security technique for 5G wireless networks and challenges ahead,” IEEE J.Selected Areas Commun., vol. 36, no. 4, pp. 679-695.

[7]. J. Heo, J. Kim, J. Paek, S. Bahk(2018), “Mitigating stealthy jamming attacks in lowpower and lossy wireless networks,” J. Commun. Netw., pp. 219-230.

[8]. Dongfeng Fang,Yi Qian and Rose Qingyang Hu(2017),”Security for 5G Mobile Wireless Networks,”digital object identifier10.1109/ Access.2017.2279146,vol.11,pp.1136.

[9]. O. Pu˜ nal, I. Aktas¸, C. J. Schnelke, G. Abidin, K.Wehrle and J. Gross(2014),“Machine learning-based jamming detection for IEEE 802.11: design and experimental evaluation,” IEEE Int. Symposium Wireless, Mobile and Multimedia Networks, pp. 1-10.

[10]. K. Grover; A. Lim; Q. Yang(2014), “Jamming and antijamming techniques in wireless networks: A survey,” Int. J. Ad Hoc Ubiquitous., pp. 197-215.

[11]. Guan, B., Yao, J., Zhang, G., Wang, X, “Thigh fracture detection using deep learning method based on new dilated convolutional feature pyramid network”, Pattern Recognition Letters vol 125, pp. 521–526, 2019.

[12]. H. Reyes, N. Kaabouch(2013), “Jamming and lost link detection in wireless networks with fuzzy logic,” Int. J. Sentific Eng. research, vol. 4, pp. 1-7.

[13]. I. Almomani, B. Al-Kasasbeh and M. Al-Akhras(2016), “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks,” J. Sensors, vol. 2, doi: 10.1155/2016/4731953.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

[14]. M. A. Alsheikh, S. Lin, D. Niyato and H. P. Tan(2014), "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Commun. Surv. Tutorials, doi: 10.1109/COMST.2014.2320099.

[15]. S. Gunduz, B. Arslan and M. Demirci(2015), "A review of machine learning solutions to denial-of-services attacks in wireless sensor networks," in Proceedings 2015 IEEE 14th International Conference on Machine Learning and Applications, ICMLA 2015, 2016, pp. 150–155, doi: 10.1109/ICMLA.2015.202.

[16]. C. Ioannou, V. Vassiliou and C. Sergiou(2017), "An Intrusion Detection System for Wireless Sensor Networks," 2017, doi: 10.1109/ICT.2017.7998271.

[17]. G. Pachauri and S. Sharma(2015), "Anomaly Detection in MedicalWireless Sensor Networks using Machine Learning Algorithms," in Procedia Computer Science, 2015, vol. 70, pp. 325–333, doi: 10.1016/j.procs.2015.10.026.

[18]. B. Riyaz and S. Ganapathy(2020), "A deep learning approach for effective intrusion detection in wireless networks using CNN," Soft Comput., vol. 24, no. 22, pp. 17265–17278, doi:10.1007/s00500-020-05017-0.

[19]. P. Nancy, S. Muthurajkumar, S. Ganapathy, S. V. N. Santhosh Kumar, M. Selvi and K. Arputharaj(2020), "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," IET Commun., doi: 10.1049/iet-com.2019.0172.

[20]. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran,Al-Nemrat and S. Venkatraman(2019), "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, doi: 10.1109/ACCESS.2019.2895334.