Detection of jamming and interference attacks in wireless communication network using deep learning technique

[1]S.V.Manikanthan, [2]T.Padmapriya
{[1]manikanthan.s.v@gmail.com, [2]padmapriyaa85@pec.edu}

[1]Director, Melange Academic Research Associates, Puducherry, [2]Managing Director, Melange Academic Research Associates, Puducherry
authors

Abstract. The Jamming and interference attacks aim to disable a wireless network, inducing a denial of service. Despite the resilience offered 5G is prone to these regarding the impact to the use of millimetre wave bands. In the last decade, several jamming detection techniques have been developed, including fuzzy logic, game theory, channel surfing, and some others statistical modeling. The plurality of these strategies are inadequate at detecting smart jammers. As a response, efficient and quick jamming and interference high-accuracy detection systems are all still in great demand. The usefulness of many deep learning models in detecting jamming and interference signals is analyzed in this paper. The types of signal features that could be used to diagnose jamming and interference signals are investigated, and a large dataset was created using these parameters. Deep learning algorithms are being kitted, tested, and sorely tested using this dataset. Logistic regression and naïve bayes are representations of these algorithms. The probability of detection, probability of false alarm and accuracy are being used to verify and validate the performance of these algorithms. The simulation results show that a logistic regression algorithm based on jamming detection and interference can detect jammers with perfect seating, a high possibility of detection, and a minimal probability of false alarm.

Keywords: jamming, interference, deep learning, logistic regression, logistic regression, jammers.

1 Introduction

In the near future, 5G is set to transform earlier generations of cellular networks by requiring superior throughput and inferior latency [1], setting the stage for “self-driving” cars, the internet of things, E-health maintenance, augmented worlds, and smart cities. As a result, billions of wireless systems are designed to be associated to the internet. Cyber threats including such jamming [2] and GPS spoofing makes 5G, like all other networks, vulnerable [3, 4]. Cognitive radio can render these risk taking to new attacks [5-8], such as main customer emulation [5] and data falsification through spectrum sensing [6]. As a result, it's crucial to understand the cyber security effects of 5Mobile communications [8,9]. Jammers create an insanely large amount of ignorance of service by overflowing communication channels to radio signals, dropping the SNR of genuine users and interrupting communication. GNU radio

I3CAC 2021, June 07-08, Chennai, India

DOI 10.4108/eai.7-6-2021.2308599

and universal software radio peripherals are representations of proposed software radio units inexpensive, can be used to launch attacks.

Jammers can readily find any frequency channel at a low cost. [10]. The four essential types of jamming attacks are constant jammers, random jammers, deceptive jammers, and reactive jammers. Constant jammers attack by sweeping a full capacity noise from one channel to the next as seen in a scheme and repeating the process over time. Random jammers operate at random, with no special method for moving from one channel to the next. To keep wireless channels distracted, manipulative jammers send illegitimate packets through them. Reactive jammers keep track of the number Also jam the channels that are used for communication out of all frequency channels [11]. Jammers could also be labeled as standard or smart. Daily jammers don't seem to be capable of distinguishing amongst continuously transmitted signals, so they all play at the same time. Smart jammers are likely to actually to understand, map, and determine how legitimate users transmit their signals, enabling them to develop their attack strategies or communication energy cause serious trouble to legitimate transmission.

The fifth-generation (5G) cellular network period is rapidly approaching. The intensity of research is growing up in the region in readiness for the first suborbital flights. 5G networks are prepared to facilitate the energy sector as well as “vertical industries” such as automated driving, smart factories, and medical care. They will also provide multi-tenancy and micro support, as well as approaches for accelerating customer service delivery and presenting computing and networking modules to service providers [1]. The prime motive is to allow operators to provide vertical service providers with handmade solutions over the same network infrastructure. Beyond these approaches, slicing a 5G network offer a wealth of mobility and support for a variety of different performance criteria. Network functions are modularized and can be installed in a number of different ways achieves this. The network programmability rule can also be extended. Network functions virtualization (NFV) and software defined networking (SDN) are manifestations of enablers [4]. Through the latter, the former enables a flexible logical architecture and versatile location of NFs in the network virtualization of NFs. The figure 1. shows the block diagram of wireless communication.

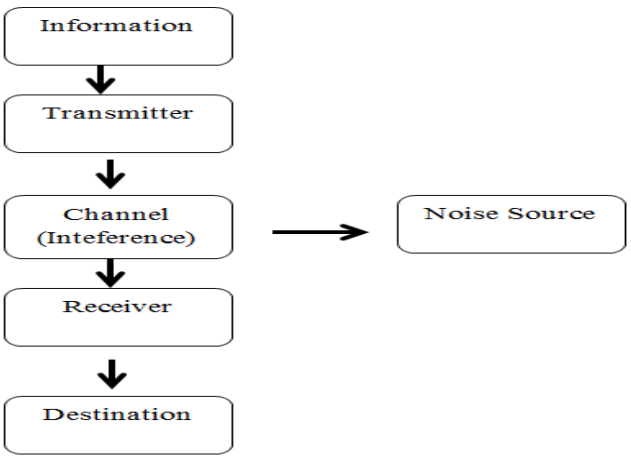

Figure 1. Wireless communication Block diagram

We live in a golden age of technology. Without knowledge, would have been unable to think for a single moment. Science has made our life easier and more relaxed. Because of the advancement of technology, the modern world is being highly compressed. Due to various science and technology, the telecommunications industry has changed significantly over the past few decades. The term "5G" refers to the fifth generation of mobile technology. The use of handheld devices within very high bandwidth has changed thanks to 5G technology. 5G is a high-throughput, wide-coverage packet switched wireless system. 5G technologies use CDMA and BDMA, as well as inch wireless, to endorse seed speeds of more than 100Mbps at full movement and more than 1Gbps at low mobility. Many types of new features were included in the 5G technology, making it the in the near future, the most efficient and in high demand. It's not incredible that such a scientific treasure exists has indeed been squeezed into such a tiny device.

Mobile phone subscribers get more features and performance to 5G technology. Many types of new features should be included in 5G technology, make it the most efficient and in high demand. It's not common with such a wide selection of technology to arise has also been jammed into such a tiny device. Mobile phone customers get even more features and performance to 5G technology. 5G is a new technology that will provide all conceivable devices with just one universal machine whereas interconnecting the majority of recent communication infrastructures. The 5G terminals will be multimode and cognitive radio efficient and portable. Software-defined radio modulation schemes is used. All of the required swappable software can be downloaded on the fly from the internet. The implementation of 5G mobile networks will be focused on the creation of user terminals, that will provide simultaneous access to the several wireless technologies and will consolidate numerous flows from various technologies. Moreover, the terminal will make the final decision among mobile network topology.

Enhanced the role for data and control transport, as well as supporting activities for tools and other technologies networks, help compensate Next generation networks (NGN). In order to provide quality of service, traffic assessment is a basic control function. Moreover, the 5G connectivity program was made with the best service in mind (QoS). The potential of a network to increasing prevalence bandwidth while still dealing quality of service refers to the integration of effective leader elements such as latency, error rate, and uptime (QoS). Setting priorities for different data sources (video, audio, files) on the network enables them to setup and share network resources sometimes component of quality of service. Just QoS corresponds to network traffic developed for video on demand, IPTV, VoIP, streaming media, videoconferencing, and online gaming. Quality of service helps to offer priority to networks by delivering enthusiastic bandwidth, jitter power, low latency, and reduced loss characteristics. Its solutions provide the foundation for emerging campus, wide area network, and service provider networks business applications [12].

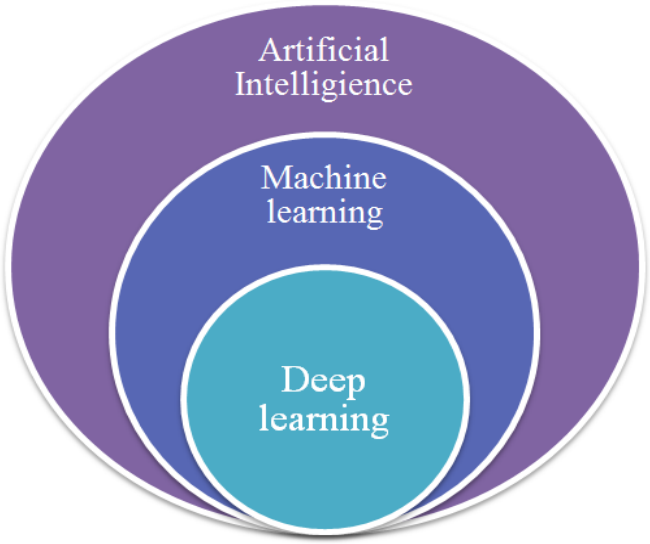

Figure 2.Deep learning in advance

5G networks are digital mobile networks that divide their frequency range into improve road cell membrane units The 5G wireless devices in a cell use radio waves to communicate with a local antenna array and low-power automated transceiver (transmitter and receiver) in the cell. The transceiver allocates frequency channels from a pool of frequencies that are reclaimed in other cells. Local antennas are related to transmission electronics, which are connected to telephone wireless equipment transmission and routers using high-bandwidth multimode or wireless backhaul connections for internet access In other cell networks, a mobile device shifting from one cell to another is seamlessly handed over to the current cell. A million devices per square mile can be enabled by 5G, while 4G can only support a tenth of that [13,14]. Since the new networks use 4G to establish the connect with the cell, and the new 5G wireless devices now have 4G LTE potential in areas where 5G coverage is not available[15]. The frequency range for low-band 5G is 600–850 MHz, which again is close to the one of 4G cellphones, which generates download speeds of 30–250 megabits per second (Mbit/s). Low-band cell towers are similar to 4G towers in respect of range and coverage area. Mid-band 5G uses microwaves between 2.5 and 3.7 GHz to provide speeds of 100 to 900 Mbit/s, with each cell tower reaching multiple miles. This is the most common form of infrastructure, and it should be usable in most large cities by 2020. Because certain low-band is the minimum service tier that regions have yet to introduce. Because, in the future, higher frequencies can be used, high-band 5G uses frequencies of 25–39 GHz, near the bottom of the infrared imaging band. It often experiences download speeds comparable to cable internet gigabit per second (Gbit/s) is a measurement for the faster data transfer. Millimeter waves (mmWave or mmW) have a wider variety, which can necessitate their use the use of several small cells.

2 Related Works:

Yifei, Y., & Longming, Z[16] explained that the increasing growth of mobile internet and the internet of things has motivated the development of 5G wireless communication systems, which are scheduled to be introduced around 2020. (IMT-2020). 5G networks are expected to offer a wide range of application scenarios. As a rule, 54 g would have a wide range of available performance metrics (KPIs), instead of the peak data rate and average/edge spectral emissions standards of previous generations. Multiple technologies can be used individually or in conjunction in each typical scenario to boost transmission quality, reduced costs, and increase the number of connections, among other factors. Huge MIMO, ultra dense application specific techniques, non orthogonal transmission, high frequency communications, and other important enabling technologies are mentioned.

The author Kaloxylos, A[17]described the 5G networks are intended to serve a multitude of vertical industries with varying performance criteria. Network slicing is found to be the major enabler for enhancing cellular networks' efficiency in order to achieve this goal. The theory of network slicing has been studied extensively in past months, and the key performance parameters have been developed. However, network slicing adds a layer of complexity that triggers several problems that are still being studied. This article includes a comprehensive overview of the things proposed by the research community, as well as the legal condition of the 3GPP simulation phase. This research looked at solutions for all network domains (access, transport, and core), as well as network slice management. The paper will also discuss significant issues which need to be resolved in the upcoming months.

According to the author Pedreira, C. E[18] explained that the method for modifying LVQ prototypes that selects a subset of the training data points. The principal goal is to have experiments converge in a more convenient venue, which could eliminate misclassification errors. Nowadays an update range made up of a subset of points that are likely to be captured by another class prototype. In order to describe different levels of importance for the input attributes, they compare the proposed technique with a weighted norm rather than on the euclidean. The method is tested in a probability sample as well as on readily viewable data sets.

Maalouf, M [19] explained that logistic regression (LR) is one of the most famous data mining methods in common and in binary data categorization in particular. This document gives an impression of the main aspects of LR in data analysis, primarily from an algorithmic and machine learning context, and how LR can also be used to analyze the data from imbalanced and irregular events.

According to the author Agiwal, M.,[20] explained that compared to current 4G LTE networks, the vision till next 5G wireless communications is to have extremely high data speeds (typically in the kilobytes per speed range), extremely low latency, a significant rise a significant increase in base station output, and a marked enhancement in perceived service quality (QoS). Established cellular networks are already being stressed by the proliferation of mobile devices, the proliferation of digital multimedia technology, and the explosive growth of wireless data (multimedia) demand and usage. Most mobile phones are anticipated to prosper by 5G wireless events, with increased download speeds, speed, latency, and QoS. In this survey, we explore the wireless evolution toward 5G networks in detail. Will suggest talking about both the latest architectural advances in radio access network (RAN) development, such as air interfaces, smart antennas, cloud, and heterogeneous RAN. Regarding that, go above the new channel model estimation, directional antenna configuration, beam formation algorithms, and large MIMO technologies underlying novel

mm-wave physical layer technologies in detail. The protocols and multiplexing schemes and for MAC layer which might represent this new physical layer are mentioned here effectively are then covered. Analyze the killer apps, who were thought to be the main driving force behind 5G. Highlight in order to further explain the enhanced customer experience, new QoS, QoE, and SON features consistent with the 5G evolution are being introduced. They receive a complete information about energy sensitivity and cost efficiency in order to reduce increased network electricity consumption and capital expenditures. They also address specific understanding the current condition of 5G technology is crucial for its ultimate commercialization, which necessarily involves field trials, drive tests, and simulation studies. Finally, the best previous researches topics were discussed, and future research directions. [20]

Huang, Z[21] described that the foundation of deep neural networks, DLVQ (deep learning vector quantization) is a modern deep learning vector quantization algorithm (DNNs). By using deep learning framework's heavy representation ability and any vector quantization (VQ)method as an initializer, the proposed DLVQ technique in a classification task, is capable of learning a code-constrained codebook and thus outshines standard VQ. When the k-means VQ technique is often used to allow the proposed DLVQ, it achieves a positive outcomes on an activity requiring audio information retrieval A 10.5 percentage point in mean average precision (MAP) is obtained after merging the k-means and DLVQ data.

According to the author Jover, R. P, et al..,[22] explained that the on a tasks requiring audio information retrieval A 10.5 percentile rank in mean average precision (MAP) is obtained after merging the k-means and DLVQ data added platform that allows additional mobility and coverage for follow new networks, which are factor loading increased traffic and the ever bandwidth criteria This new cellular communication system, which uses an orthogonal frequency division multiple access (OFDMA) modulation and is based on a revised physical layer, functions well here in multipath environments and increases the wireless channel's system efficiency in terms of bits per second per Hertz (bps/Hz). Nonetheless, LTE is vulnerable to radio jamming attacks, as are all wireless systems. Such threats prove to be dangerous, especially for based on LTE networks, next-generation emergency response communication systems.

His proof-of-concept study sets out a bunch of short major attacks (smart jamming) that broaden the range and effectiveness of radio network jamming. Focused on these new risks, a number of new possible safety research directions are suggested, with the intent of enhancing the resiliency of LTE networks against such attacks. The primary downlink broadcast channels are spread-spectrum controlled, with the uplink control channels' radio resource allocation distorted and a standard cryptographic scheme for process information messages. Despite the challenges of incorporating these technologies on commercial networks, which would necessarily require their inclusion in future LTE standard launches, the technology solutions have the potential to significantly improve the performance of LTE-based national emergency response communication systems.

3 Proposed Work:

Many other types of artificial neural networks, supervised or unsupervised learning techniques (ANNs), are being used in deep technologies to learn hierarchical embodiments. There are a range of DL architectures that have been made up largely of several layers of processing. Each layer can create non-linear responses based on the data from its input layer.

Human structures emulate DL's usability. Signal process is done by the brain and tissues. In relation to other previous techniques to machine learning, DL architecture has gained more attention in recent years. DL Architectures are treated as shallow-structured forms of such approaches (i.e. a small subset). While ANNs have had a considerable rise in previous centuries, DNNs beginning in 2006, when. presented the emergence with networks of deep ideologies. This technology's state-of-the-art quality was extensively documented. Image recognition, image recognition, retrieval of search engines and information, and natural language translation are all areas of AI. Training data was another contributor to collinearity on the miniature scale. The implementation of successful deeper exploration was prohibited in those days with FNNs due to action and computer production capacity.

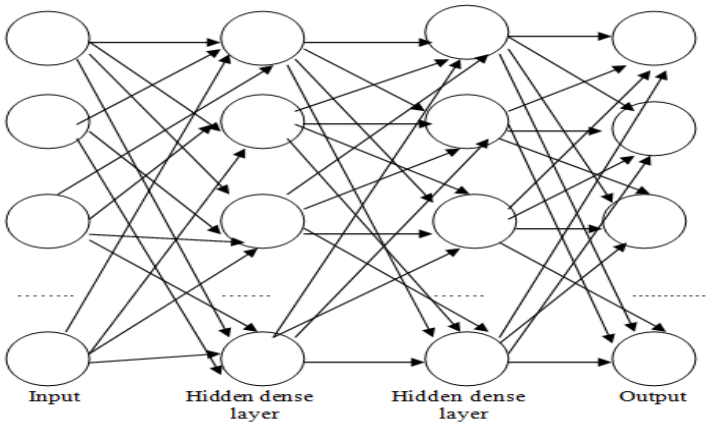

Figure 3. The overall mechanism of deep learning

The systematic propagation radio jamming the use of radio signals to disturb communications by decreasing the SNR of the received signal. This assault generally requires sending a persistent high-power signal through the entire target band of the system being assaulted. This attack is largely viewed as a transparent and simple method of disrupting a wireless network, and it has been thoroughly studied in the literature in the environments of wireless local area networks (WLAN)[4], sensor networks, and cellular networks. Detecting and countering the hacker, despite the attack's simplicity, is often the only alternative, particular when the device's entire band is jammed. More advanced schemes to jam cellular networks are being proposed, spite of the fact that the huge portion of transmitted power destroys stealthiness. When the attacker is aware of the target signal, a regular barrage jamming attack has been shown to be the most powerful jamming method. Downlink smart jamming head straight forth malicious radio signals to impede the processing of vital downlink control channels. A new study discusses the social ramifications of jamming LTE networks' PBCH. The central contention built on the questions in the study. This attack, can be used on this channel is approached by both 2G and 3G networks although its designated PRBs are established long in advance and are always mapped to the central 72 subcarriers of the OFDMA signal, as mentioned. Attributed to the reason that this channel has been used to configure and operate the other channels in the cell, this jamming attack seems to have a low duty cycle and bandwidth. The figure 2. shows the mechanism of the deep learning.

In this case, the jammer's range is still very reduced, with a very limited effect. To deny treatment to non-cell edge users, the PBCH's Through this, transmission and modulation features necessarily require a largish interfering signal. Remember that the attacker's potential to out power the legitimate signal is constrained by the e Node B's large transmitted power and the jamming device's potentially low transmitted power. Smart jamming with low power goes a step further by jamming uplink control channels that really are essential to the platform's service. An uplink smart jamming attack has a greater variety, cover the entire cell or business. Although the hacker jams the UL systems node B seems unable to accept important UL transmitting messages needed for the cell's correct functioning. The attacker actually blocks the by overwhelming reception at the e node B with a jamming signal, the base station is blocked from interacting with any UE in the cell, increase the the attack's range looks at the entire cell. Furthermore, the attacker is constrained not by the high power of the downlink signals by Node B (which are often in the 48 dBm range), but by the maximum power that a legal UE can transmit, which is set to 23 dBm in the case of LTE. An offender sitting opposite node B and transmitting at the same power level as any legitimate smartphone can possibly jam all of the UEs in a cell or sector's uplink control messages in this circumstance. Furthermore, the attacker that decide to use an extremely targeted antenna guided at the node B to substantially boost the attack's effectiveness.

After the first data exchange on this channel helps the UE to organize in the uplink, radio resources can be allocated to the UE after the initial delivery results. A hacker will have to understand the precise PRBs per each LTE uplink control channel at the PHY layer in order to target it. Readily viewable information can also be used to obtain this PRB assignment. Yet the, even when the simply raise of the these though data about radio resource assignment could not have been got from the SIB unprotected data’s carried by the PBCH and PDSCH although signals in the time-frequency LTE frame was unpredictable or scrambled, data about radio resource assignment could still be gained from the SIB unprotected messages handled by the PBCH and PDSCH.

In the SIB-1 text, the MCC and MNC of an e node B are also encoded, which is important to note in the background of a sophisticated and extremely targeted attack. If this information is obtained, a hacker may, for example, target base stations from a various biological network operator with the jamming cost. Though far more efficient than straightforward jamming or downlink smart jamming, uplink smart jamming is a further complex operation. To selectively jam the PRBs delegated to, say, the RACH channel, an intruder must've been perfectly time and frequency compatible with the LTE signal. Thirdly, the attacker must of been able to decrypt and decode MIB and SIB messages in order to take out the actual RACH PRB allocation information. A professional attacker and reasonable progress work on software-defined radio, for example, may be used as a response, will be necessary.

4 Logistic Regression:

The the probability of assigning observation x to prototype j, p (j | x), is equivalent to their (Euclidean) size, which is the starting point for Regression LVQ (RLVQ) algorithms. Assume that a mixture model could describe the probability density b (x) of x.

$b(x) = \sum_{i=0,1,2.3}^{a} p(x|k)$ (b(i)) (1)

where b(i) is the conditional probability that component j generates particular data point x, and is the prior probability that a data point is generated by a single component.

Should use the condensed exponential form to reflect the conditional density function p (x | k).

$p(x|k)$ = K(i). exp (f(x, y_j)) (2)

and even a Gaussian mixture of K (j) = (2 p 2)1/2 and f (x, mj) = (x mj)2 / 2p2. Component j is absolutely described in this case by its mean mj and standard deviation p. As a response, component j can be identified as prototype j, and I will proceed to use such a convention in the journal. It's worth mentioning that the standard deviation (width) of all concepts was presumed to be the same. Assume whether p(j) = 1/P is the same for all designs. Given this, the assignment probability can be reported using the Bayes law.

P (x | k) = exp(-(z - y_j)^2 / 2δ2$_m$) (3)

Let X∈R^{n*d} be a data matrix for n instances (examples), d features (parameters or attributes), and y a binary outcome vector either y_i = 1 or y_i = 0 is the output. Within each instance x_k∈ Rd (a row vector in X), where I = 1...n, y_k = 1 or y_p = 0 is the result. Let instances with yk = 1 be positive (an event happens), and instances with yp = 0 be negative (an event doesn't really occur) (non-occurrence of an event). The step is to predict whether xi is a positive or negative example. A case can be thought of as a Bernoulli trial (the random component) with an expected value E[yk] or probability pi. In able to fix such a problem, the systems approach will be used in a linear regression model.

$M = X\gamma + \tau$, (4)

Where τ is the error vector,

$$Z = \begin{pmatrix} x1 \\ x2 \\ x3 \\ \vdots \\ xn \end{pmatrix} \quad (5)$$

$$L = \begin{bmatrix} y11 & y12 \ldots. & y1d \\ y21 & y22 \ldots.. & y2d \\ yn1 & yn2 \ldots. & ynd \end{bmatrix} \quad (6)$$

$$\alpha = \begin{pmatrix} \alpha 1 \\ \alpha 2 \\ \alpha 3 \\ \vdots \\ \alpha d \end{pmatrix} \quad (7)$$

$$\sigma = \begin{pmatrix} \sigma 1 \\ \sigma 2 \\ \sigma 3 \\ \vdots \\ \sigma d \end{pmatrix} \quad (8)$$

The vector is a range of unknown parameters only with parameters xi← [1,xi]. From now on, the intercept will be believed to be implemented into to the vector Now, since y is a Bernoulli random variable with a probability distribution, now let us peek at it, let's peek at it.

$$P(b_i) = \begin{Bmatrix} Gi, \text{if } yi = 1 \\ 1 - b, \text{if } yi = 0 \end{Bmatrix} \quad (9)$$

the response's expected value is then

$$E[k_i] = 1(g_i) + 1(5-p_i) = g_i = x_i\omega, \quad (10)$$

with a variance,

$$V(y_i) = k_i(1-k_i) \quad (11)$$

It follows from the linear model

$$x_i = x_i\alpha + \varepsilon_i \quad (12)$$

that

$$\beta i = \begin{cases} 1 - pi - 1; \text{ if } yi = 0 \text{ with probability pi} \\ -pi; \text{ if } yi = 0 \text{ with probability } 1 - pi \end{cases} \quad (13)$$

As a function, $\in$I has a binomial distribution with an investor participation.

$$E[\gamma i] = (1-a_i)(b_i + (-b_i)(1-a_i) = 0, \quad (14)$$

$$V(\varepsilon i) = E[\varepsilon^2 i] - E[\alpha i] = (1-bi)^2(pi) + (-bi)^2(1-pi) - (0) = ai(1-bi) \quad (15)$$

The least squares solution should be used since the obtained value and variance of the result and error are not constant (heteroskedastic), and the errors are not normally distributed After this, since y_i = 0,1, a linear regression model can give results that are above or below zero. The logistic response function is a function that helps you to quickly respond to, as shown in figure 2, is the acceptable one when the response vector is binary.

5 Attack complexity:

To selectively jam the RACH, the attacker would need total correlation in time and frequency with the LTE signal, per the characteristics of UL smart jamming. In relation to DL smart jamming, this enhances the attack's sophistication. However, there are a range of the off

and open-access resources which could be used in this scenario. By jamming the central 1.08 MHz of any LTE signal, an attacker may deny service to all UEs in its vicinity. As a rule, it's critical to improve the primary broadcast channels' PHY layer stability. The objective is to counteract the jammer's advantage in bandwidth and transmitted power in the form of the LTE limitation. New LTE networks employ a completely revamped modulation scheme that greatly enhances the wireless channel's overall performance of bits per second per Hertz (bps/Hz).

6 The Proposed Basic Jamming Detection Method:

In this method, in order to build an application, machine actions are listed. Abnormalities in the sensor network and the introduce unique profile. By comparing later profiles, you'll be able to figure out what they're doing. During setup process, the initial parameter levels (PDR, BPR, and ECA) are sampled, and it is expected that no jammer will disturb the sensor network. The threshold levels all of which were sampled and documented are later used to indicate the existence of any jammer. The threshold concentrations were assessed using the 6-Sigma procedure, which is a simple and effective calculation technique. By using arithmetic mean and standard deviation values, the UCL (Upper Control Limit) and LCL (Lower Control Limit) limits of normally distributed samples can be determined. The arithmetic mean is represented by and the standard deviation is represented by 99.999660 % of the data in normally distributed outputs is between the UCL and LCL limits. The balance of the data set is marked as normal as it falls just below LCL or approaches the UCL. PDR threshold parameters are compared to use the LCL, although BPR and ECA threshold levels are estimated using the UCL. The pseudo codes for the basic jamming detection mechanism, which compares documented parameter threshold values to periodic measures of these parameters. Five-branched if-else terms are also used to classify attacks and fault events. Each branch is aligned for one or more attack styles or fault circumstances. When instant PDR is lower than the threshold value (PDR) The, instant ECA is higher than the threshold, and instant BPR is higher than the threshold, a sensor node is admitted under attack in the first request city code.

When sensitive or inaccurate threshold samples are used, the detection mechanism may deliver inaccurate results. As a results, under these abnormal and unexpected network conditions, the basic jamming detection mechanism will lead to lower detection quality and increased false positive rates. There are also instances if an attack or a failure in the sensor network cannot be easily remedied. Node-A (the boundary node) is not openly threatened by a jammer, but it is influenced indirectly by nearest neighbours. In this case, and although PDR decreases, the ECA and BPR values can be maintained within reasonable parameters. This issue may also emerge as a result of neighborhood node failures. As a rule, the attack and fault cases in the boundary nodes cannot be removed easily in the specific detection mechanism.

7 The Proposed Advanced Jamming Detection Method:

Because of the limitations of the basic detection mechanism listed above, an advanced jamming detection mechanism is required. Another supplementary approach is needed to help threshold technique in order to achieve higher detection rates with lower false positive rates.

In the advanced mechanism, the parameters used in the standard jamming detection method are paired with additional network query packets to construct a query-based jamming detection method. The advanced detection methodology uses not only the relationship amongst sampled parameters within the same node, but also the parameters of neighbouring nodes. When abnormal network parameters (($PDRPDR_{The}$ && $ECA>ECA_{The}$) || ($PDRPDR_{The}$ && $BPR>BPR_{The}$)) are sampled, it is centered on exchanging QUERY and REPLY packets between nearest neighbors. When a sensor node is in a suspicious state, it sends out QUERY packets with the ALARM flag set to sense the amount of an attack. The nodes that receive the QUERY packets analyze their network parameters and set or clear the If any variations are identified, an ALARM flag is set in the REPLY packet. In the QUERY-REPLY, the Alert flags packets can be used for the nodes to indicate the existence of a possible attack. The tabulation 2 and 3 shows the probability values using logistic regression and nave Bayes algorithm

S.No	Probability of detection	Probability of false alarm	Probability of accuracy
1.	185	150	110
2.	170	182	150
3.	135	147	163
4.	149	151	189

Table 1. The values of probability using logistics regression

S.No	Probability of detection	Probability of false alarm	Probability of accuracy
1.	142	166	179
2.	139	147	154
3.	99	120	167
4.	180	110	128

Table 2. The values of probability using Naïve Bayes

Algorithm-2, which is shown below, introduces the advanced detection. Every sampling cycle, the device is called query based jamming detection Algorithm, and it requires use of such external variables flags to evaluate how or not an attack occurs. When an abnormality is identified, a QUERY procedure is initiated. To mitigate QUERY-REPLY packet traffic between nodes in the same community, the node receives a QUERY packet could indeed postpone sending the before sending the QUERY packet, wait for the REPLY project to finish before sending it. If the number of REPLY data packets is less than planned, the node sends a QUERY packet. Otherwise, the node does not send a QUERY packet but instead focuses on received REPLY packets to indicate the location of an attack. By implementing the contention protocol rules, the node that hasn't really received a QUERY packet before sending the QUERY packet must send the QUERY packet in three sampling times. If the node becomes unable to send any QUERY parcels and within specified it is believed that the channel is operated by during that time persistent or malicious jammers. The node that carries out the

QUERY packet waits for the REPLY packets to arrive within a certain length of time. When the QUERY-REPLY tournament starts, the nodes inspect the REPLY packets to see whether there is any indication of an attack. The presence of a jammer is decided by nodes.

//Called upon each sampling period
Query based jamming detection algorithm(){
if ((PDR<PDR_{Thr} **AND** ECA>ECA_{Thr}) **OR** (PDR<PDR_{Thr} and BPR>BPR_{Thr})) *//Abnormality*
if(Rcvd query=**FALSE AND** waiting reply for other nodes=**TRUE**)
set reply timer(Now+5*sampling period)
Waiting reply for others=**FALSE**
else if (waiting reply for others=**FALSE AND** query timer overflow=**TRUE**
Evaluate reply packets();
else if(rcvd query=**TRUE AND** waiting reply For other nodes=**TRUE**)
if (Trying to send query=**FALSE**)
try to send query packet();
Set query timer(now+2*Sampling Period)
trying to send query=**TRUE**
else if(query timer overflow=**TRUE AND** query was sent=**TRUE**)
Cancel Query Timer()
set reply timer(Now+3*Sampling Period)
else if (Query timer overflow=**FALSE AND** Query was sent=**FALSE**)
JAMMING=FALSE;
if(Number Forced Query<3)
Send forced query(now+ random time)
Forced query was Sent=**TRUE**
Number forced Query++
end if
else if(Reply timer overflow=**TRUE**)
Evaluate reply packets();
else if (PDR<PDR_{Thr} **AND** BPR<BPR_{Thr} **AND** ECAn<ECA_{Thr} **AND** Rcvd forced query=**FALSE**) *// Boundary Nodes*
JAMMING=TRUE;
else if(PDR<PDR_{Thr} **AND** BPR<$BPRT_{hr}$ **AND** ECA<ECA_{Thr})
FAULT=TRUE;
else
JAMMING=TRUE;
end if
end if
end if
}

Some special properties are needed for boundary nodes in the detection to jamming under constant, listen interval, and control interval jammers. For boundary nodes, which are located on the outside of a jammer's coverage area, the PDR, BPR, and ECA parameter levels will be low. Neighbor node failures also may allow these parameter levels to appear. As a practice, it's easy to blend up an intrusion scenario and a fault scenario. The nodes use FORCED QUERY packets to solve this limitation in the proposed advanced detection phase. If a node can't even send out any QUERY packages in that amount of time, it considers itself jammed and waits

for a random time to send out a FORCED QUERY packet, ignoring contention protocol rules. As a rule, the boundary nodes receiving the FORCED QUERY packet are better able to distinguish between fault and jamming instances.

8 Naïve Bayes:

Have a hypothesis in Bayesian classification that the given data belongs to a specific class. The possibility of the hypothesis proving valid is then measured. For some types of problems, this is one of the most practical solutions. The method only generally requires a standard scan of the entire data. Thirdly, if additional training data are available at any level, each training example will incrementally increase or lessen the probability that a hypothesis is accurate. As a response, a Bayesian network is used to model an unpredictable domain. Evaluate the probability of an end result given multiple relevant data variables in this model. The probability of the end result, and the probability of the data variables occurring if the end result occurs, is encoded in the model. The likelihood of one evidence variable happening in the existence of the end result is assumed to be independent of the probability of other evidence variables occurring in the absence of the end result. Now we'll use a nave Bayes classifier to look at the alarm example.

Assume have a series of examples that monitor things like whether it's raining, whether an earthquake has occurred, etc. The nave Bayes classifier is premised on the idea of strong independence. This indicates that the likelihood of one attribute has really no bearing on the significance of the other. The nave Bayes classifier creates 2n from a range of n attributes! assumptions that really are irrelevant. Nonetheless, the nave Bayes classifier's tests are often correct. The study discussed in explores why and under what situations the nave Bayes classifier performs well. The error is caused by three factors, according to the report: noise, bias, and variation in training data. The best way to reduce training data noise is by using good training data. The machine learning algorithm must divide the training data into two groups. Bias is the error characterized by increased groupings in the training results. And variance is the error induced by the small groupings.

9 Results:

The results The detection rates and false positive rates of the proposed advanced jamming detection algorithm, which has been adopted, are evaluated. The tracking rates for different types of jammers and different periods of jammed nodes. The first and most significant thing to note from the data is that, while the detection rates appear to be high, they are not yet at 100%. As a result, the jamming detection method in query cycles cannot be run for all six time intervals. The second interesting issue is that as the amount of jammed nodes increases, so too does the rate of detection. This situation is exacerbated by a decrease in the number of boundary nodes. Another essential thing to consider is that in the case of complicated relations, higher detection rates are likely (lossy connections, congested or faulty sensor nodes). The rate of QUERY-REPLY packet corruption rises, and it will have a beneficial affect on the detecting rate achievement. Checking and pulse jammer scenarios had lower detection rates than the others. This is attributed to the reason that they are not successful

enough to totally occupy the communication channel, and they assault the sensor network at unexpected times. The figure 2 and 3 shows the graphical representation of jamming and interference using logistics regression and nave Bayees algorithm.

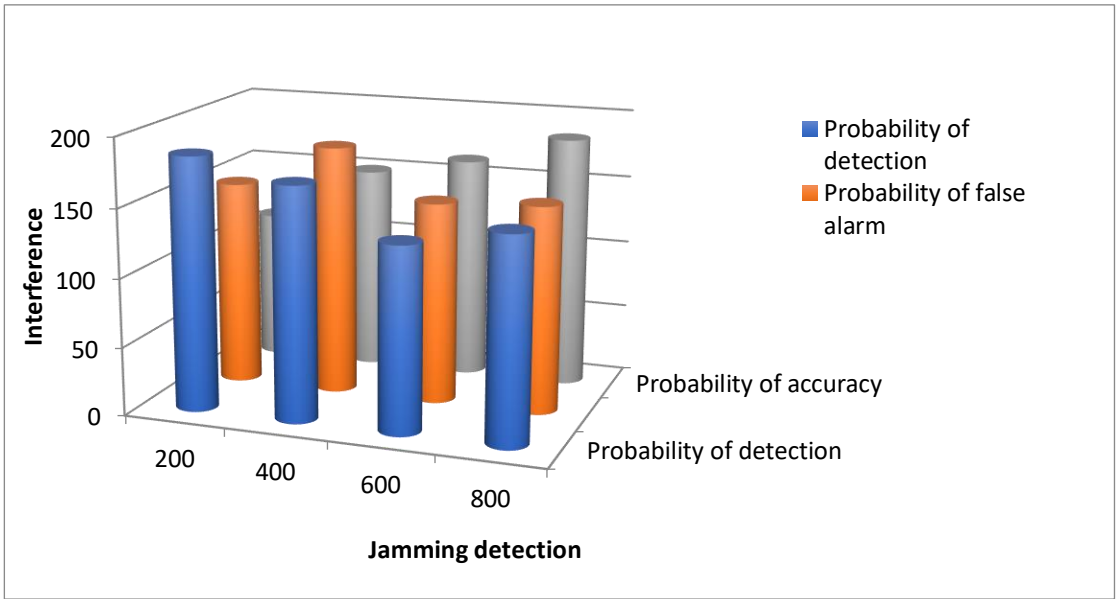

Figure 2. Graphical representation of Jamming detection and interference using logistics regression algorithm

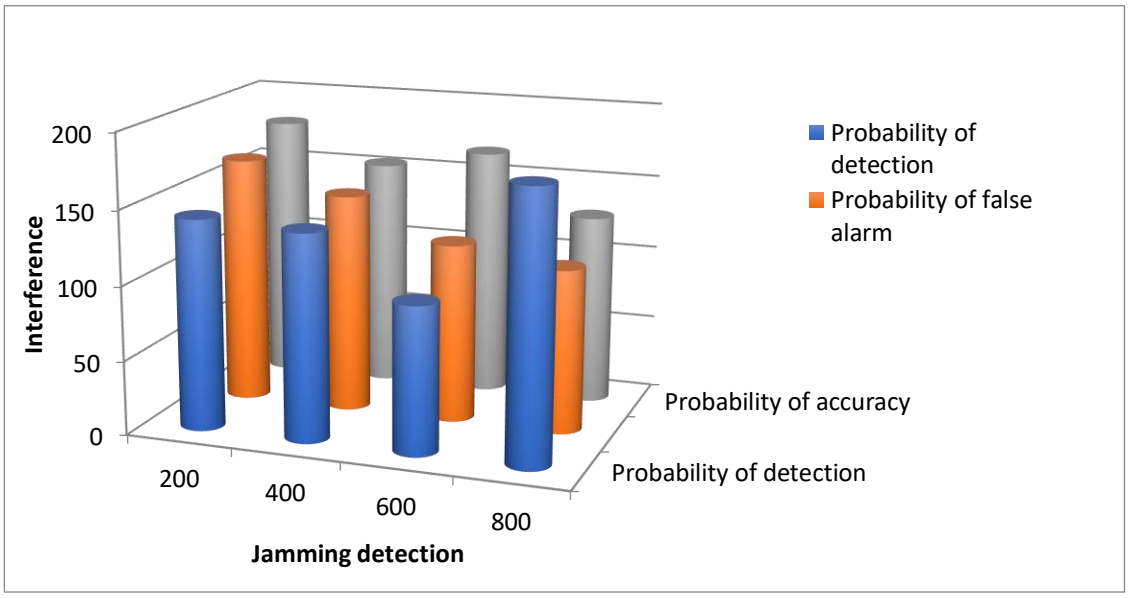

Figure 3. Graphical representation of Jamming detection and interference using Naïve Bayes algoirthm

The rates of true reports for various forms of jammers with different speeds of jammed nodes. As compared to traditional network conditions in a bad communication condition, higher positive rates can be achieved. The objective of this situation is to decrease the PDR and, on the other arm, raise the BPR. Furthermore, defective nodes in the sensor network may increase the false positive rate. Another important thought is that as the coverage area grows, the frequency of exploitable vulnerabilities decreases. The number of nodes detecting false positive conditions decreases as the number of specifically jammed gets larger. If the Jammed Node Ratio (JNR) is zero, the network doesn't even have a jammer. As a result, the false positive rates in four various graphs are comparable. Unreliable attack detections sampled from non-jammed nodes can be accepted with false positive rates sampled at nonzero JNR values.

Conclusion:

One of the most common methods of security attacks that mobility networks face is jamming. This hazard is intrinsic in the wireless devices used in this kind of network, and there is no method to deter a suspect from sending a high-power intrusive signal on a viable frequency band in its purest terms (barrage jamming). Despite the fact that jamming attacks are famous and have been carefully investigated in the literature, no actual security or mitigating measures have been enforced techniques to improve the resiliency of mobility networks against jamming attacks have been introduced. As a result, a list of latest tapping sophisticated DoS attacks against cellular networks concepts is increasing significantly. However, for the newly announced LTE advanced updates, proper settings did not list any anti-jamming recommendations or standards. Nonetheless, since LTE-based systems are expected to be enough to introduce national disaster response networks, LTE's reliability and security criteria are essential. Utilizing ideas from spread spectrum modulation, a proposed strengthening of the major DL broadcast channels' anti-jamming properties protect the wireless interface from a smart jamming attack aimed at such control channels.

References

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao, “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, 2018.

[2] D. Karas, G. Karagiannidis, R. Schober, “Neural network based PHY-layer key exchange for wireless communication,” IEEE Int. Symposium Personal, Indoor and Mobile Radio Commun., pp. 1233- 1238, 2011.

[3] P. Sinha, V. Jha, A. Rai, B. Bhushan, “Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A Survey,” Int. Conf. Signal Proc. Commun., pp. 288-293, 2017.

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

[5] M. Bouabdellah, E. Ghribi, and N. Kaabouch. "RSS-Based Localization with Maximum Likelihood Estimation for PUE Attacker Detection in Cognitive Radio Networks." IEEE International Conference on Electro Information Technology (EIT), pp. 1-6, 2019.

[6] I. Ngomane, M. Velempini, S. Dlamini, “The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks,” Info. Commun. Techn. Society Conf., pp. 1-5, 2018.

[7] M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey." Journal of information security and applications 38 (2018): 40-49.
[8] W. Alhakami, A. Mansour, G. Safdar, “Spectrum sharing security and attacks in CRNs: A review,” Int. J. Advanced Comput. Sci., vol. 5, no. 1, pp. 76–87, 2014.
[9] F. Salahdine, N. Kaabouch, “Social Engineering Attacks: A Survey,” Future Internet J., Vol. 11, No. 89, pp. 1-17, 2019.
[10] D. Fang, Y. Qian, R. Hu, “Security for 5G mobile wireless networks,” IEEE Access, vol-6, pp. 4850-4874, 2017.
[11] R. Pietro, G. Oligeri, “Jamming mitigation in cognitive radio networks,” IEEE Netw., vol. 27, no. 3, pp. 10–15, 2013.
[12] Hossain, S. (2013). 5G wireless communication systems. American Journal of Engineering Research (AJER), 2(10), 344-353.
[13] Shatrughan Singh (March 16, 2018). "Eight Reasons Why 5G Is Better Than 4G". Altran. Archived from the original on May 25, 2019. Retrieved May 25,2019.
[14] Forum, C. L. X. (June 13, 2019). "1 Million IoT Devices per Square Km – Are We Ready for the 5G Transformation?". Medium. Archived from the original on July 12, 2019. Retrieved July 12, 2019.
[15] Segan, Sascha (December 14, 2018). "What is 5G?". PC Magazine online. Ziff-Davis. Archived from the original on January 23, 2019. Retrieved January 23,2019.
[16] Yifei, Y., & Longming, Z. (2014). Application scenarios and enabling technologies of 5G. China Communications, 11(11), 69-79.
[17] Kaloxylos, A. (2018). A survey and an analysis of network slicing in 5G networks. IEEE Communications Standards Magazine, 2(1), 60-65.
[18] Pedreira, C. E. (2005). Learning vector quantization with training data selection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(1), 157-162.
[19] Maalouf, M. (2011). Logistic regression in data analysis: an overview. International Journal of Data Analysis Techniques and Strategies, 3(3), 281-299.
[20] Agiwal, M., Roy, A., & Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 18(3), 1617-1655.
[21] Huang, Z., Weng, C., Li, K., Cheng, Y. C., & Lee, C. H. (2014, May). Deep learning vector quantization for acoustic information retrieval. In 2014 IEEE international conference on acoustics, speech and signal processing (ICASSP) (pp. 1350-1354). IEEE.
[22] Jover, R. P., Lackey, J., & Raghavan, A. (2014). Enhancing the security of LTE networks against jamming attacks. EURASIP Journal on Information Security, 2014(1), 1-14.