International Journal of Robotics and Control Systems
Vol. 2, No. 4, 2022, pp. 618-627
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

An Examination of the Secure Chaos of 5G Wireless Communication Based on the Intelligent Internet of Things

Janan Farag Yonan [a,1,*]

Ministry of Higher Education and Scientific Research, Baghdad, Iraq
jananfarag@gmail.com
* Corresponding Author

ARTICLE INFO

Article history
Received June 30, 2022
Revised August 12, 2022
Accepted September 19, 2022

Keywords
Deep learning;
Intelligent-IoT;
DNN;
WSN

ABSTRACT

The implementation of an intelligent system for network control and monitoring that is built on an Internet of Things (IoT) is a focus of this line of research, with the end objective of improving the level of precision inside the network and its applications. You did indeed read it correctly; the system that is being referred to here is a deep neural network. The manner that it is constructed makes it possible for the layer that cannot be seen to contain more data. The application of element-modified deep learning and network buffer capacity control helps to improve the overall service quality that is provided by each sensor node. One method that can be applied to the process of instructing a machine to pay more attention includes deep learning in its various incarnations. The team was able to do calculations with a precision of 96.68 percent and the quickest execution time, thanks to the usage of wireless sensors. Using a sensor-based technique that has a brief implementation period, this piece has a degree of accuracy of 97.69 % when it comes to detecting and classifying proxies, and it does so using a method that is very efficient. On the other hand, our research represents a significant leap forward in comparison to earlier studies due to the fact that we were able to accurately identify and categorize a wide variety of invasions and real-time proxies.

1. Introduction

Sensor networks (WSN) report incidents to a central base station using the Ad hoc network design (BS). Fast IoT communications can be achieved [1][2] through the use of a WSN and smart technology. In order to alleviate bottlenecks in the network, a WSN that incorporates IoT must, as a matter of necessity, assign varying degrees of importance to the various categories of data [3][4].

Devices connected to the Internet of Things (IoT) play an important part in the process of monitoring an area. In this process, multiple IoT nodes process data and send it to a gateway or the cloud for further examination. The increased cost of transferring data in several dimensions can be expected (such as videos or time-series data). IoT networks that have limited bandwidth and low-power devices may have difficulty handling significant data rates. In addition to [5], machine learning (ML) and deep learning (DL) technologies can be used to enhance an IoT's intelligence (IoT). IoT network resource management is a major problem that can be solved with the use of machine learning and deep learning [6].

For human-environment interaction, new apps that leverage deep neural networks on IoT devices could be created [7]. Recent years have seen a rise in the usage of (DNNs) as controllers (DNNs). The primary goal of this paper is to create an intelligent framework [8]-[10].

2. Literature Review

Sensor-integrated IoT devices capture a lot of data. Keeping track of such a large volume of data will be a major challenge. Both options will be discussed in this section. Choosing the right DNN controller for I-IoT network congestion is the first question, and the second question is how to do it. A DNN-based clustering method would be preferable to the traditional approach described in [11, 12]. This section provides the most recent research on the use of deep neural networks (DNNs) in diverse applications.

In order to boost the capacity of a mobile show's channel, DNNs were used as a component of the channel capacity information. Guo et al. [13] attempted to increase DNN bandwidth. DNN technology and signal strength optimization was recommended by Mukherjee and colleagues [14] to improve QoS and network security in the industry IoT network. The DNN framework gains a significant amount of power by incorporating recurrent feedback. According to Mou et al. [14], (ReDNN) was developed with the intention of teaching itself how to comprehend the spectral, spatial, and temporal aspects of a picture. Images obtained by remote sensing were used for the investigation of this structure. Sonny et al. [15] suggested that CSI and DNN constructed on (LTE) should be used for parking in order to lessen the amount of traffic congestion.

Deep recurrent neural networks (RNNs) and wireless sensor networks (WSNs), as demonstrated by Belmonte-Hernández et al. [16], have been found to be able to improve the estimation of position gathered by wireless sensors in an indoor setting. Concurrent Repeated Convolutional Neural Network (CRCN) is a piece of technology that Yang et al. [17] developed for use with mobile IoT and sensors (PRDNN). In addition, Zhang et al. [18] suggested a hybrid DNN/RNN technique that is superior to DNN in terms of determining the salvage value of predictive health management technology [19]. A significant number of researchers are now striving to sharpen the focus of NNs.

To give one illustration, each RNN neuron in a layer can receive a boost from a straightforward effective called EleAttG, which can be utilized to train an RNN block. In order to increase wireless fingerprinting localization performance, Bai et al. [19] developed the DL-RNN model, which makes use of two recurrent neural networks (RNNs). Researchers have come up with a variety of ways to improve the DNN's capacity to focus during training [16][18][19]. I-IoT networks benefit greatly from the adoption of clustering techniques to reduce network congestion.

CCR, invented by Mohammed et al. [20], is a protocol designed to decrease network congestion. In order to achieve the QoS requirements of prolonging the network's life and sending more packets, the protocol was designed. Prioritizing high-priority traffic over low-priority traffic is a benefit to overloaded networks.

In MIMO sensor networks, the cluster head (Fig. 1) identification strategy was solved using Back Propagation Networks by Mukherjee et al. [21] (BPNN). While the old model had lower error rates and longer calculation times, the new one was more energy efficient. For example, network flow capture formats, tools, and methodologies are offered as a consequence of [22].

Network security monitoring and incident response are covered in detail as well as network topologies and sensor placement are explained in great detail. The most frequently used tools are explained and shown [23]. Identify network anomalies and vulnerabilities at various tiers by presenting several feature selection algorithms. Among other things, they explore the evaluation of network anomaly recognition systems as well as propose different tools [24].

In this article, we will explore various methods for analyzing experimental data, analyzing traffic behavior, acquiring data through the use of sensors, and mapping networks with Python. In addition to that, he discusses a range of methods that can be used to view network data [25].

A network proxying internet system's needs are described, as is the bro network monitor's structure and operation. The philosophy of separating mechanism from the policy in this study [26], despite its age (it was published more than two decades ago), has served as an inspiration for our research effort because it incorporates basic features of network security monitoring.

It is important to reduce the commonly used 41 features from the KDD dataset only to 16 features in order to get equal detection results while reducing the number of features. Several methods, including Weight via Maximum Relevance (WMR), Regression Analysis, as well as Stability Selection, are included in this category, were employed to narrow the results. In addition to Support Vector Machines (SVM) [27], the Bayes Classifier was employed for validation. An important takeaway from this study was the encouragement to reevaluate the value of highly detailed extracted features and the suggestion that simpler feature sets can yield better results.

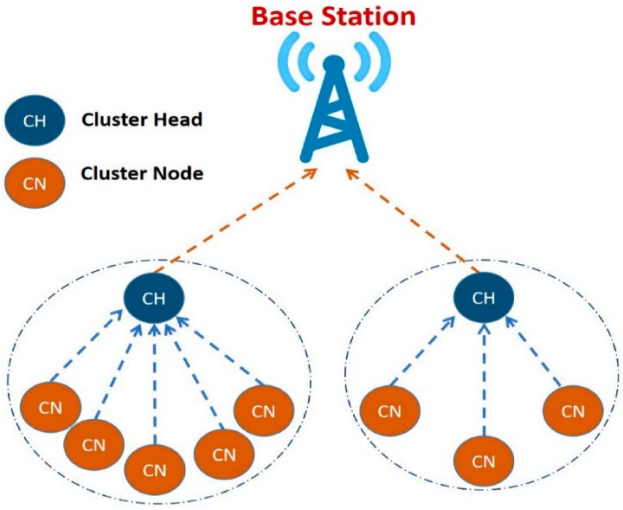

Fig. 1. A two-cluster head base station with a number of cluster nodes [28]

For large-volume network traces (Fig. 2), the packet extraction tool was tested and compared to existing methods for performance. Although their implementation could have been of considerable interest to the research community, it appears that they have not disclosed it. We were motivated to publish my entire toolchain because their results couldn't be reviewed, and future research would have to continue using inefficient tooling. Therefore, we wanted to help future researchers and allow independent verification of my results [29]. Analysis of the sculpture's governance for traffic flow testing, as well as a comparison of commonly used tools and capture formats, was presented. An excellent introduction to flow-based data collection [30].

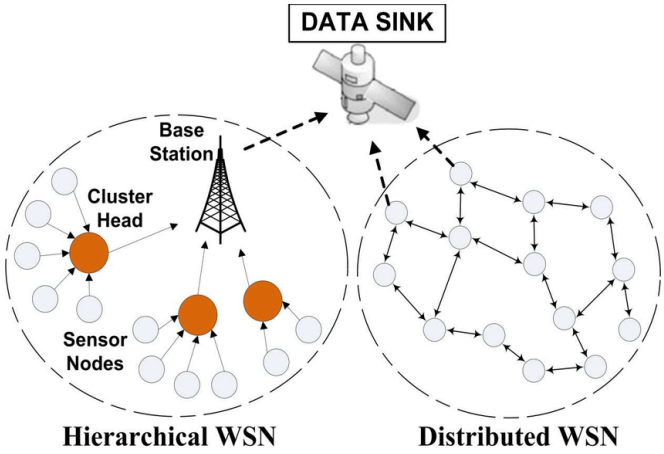

Fig. 2. Hierarchical and distributed WSN conceptual models are compared [31].

3. Deep Learning (DL)

There are two types of neural networks (ANNs) that can be used to learn hierarchies' representations of deep technologies, supervised and unsupervised. Many distinct DL designs are included in multi-layered processing architectures (Fig. 3). Non-linear responses can emerge for each layer based on the input layer's information. DL's functionality is mimicked by human methods. The brain and other neural structures are examples of materials that process signals. In recent years, interest in DL architecture and other types of generic logistic regression has grown. These strategies are regarded as shallow variations by DL Architectures. The number of ANNs increased dramatically in 2006, but the number of DNNs has increased dramatically over the prior decades, beginning with the revelation that there were deep ideological networks in existence. The most recent zenith of this technology's efficacy has been consistently reaffirmed over the years. In other fields, AI is commonly used for the translation of natural language and recognition of images.

The tiny size of the training data was another issue that contributed to collinearity. Until recently, it was unlawful to use the computational capacity of FNNs to do more in-depth research that could lead to groundbreaking discoveries. Computer hardware improvements in gpus (GPUs) and broad sensing accelerators for hardware have surpassed the coding restrictions of today's systems. In addition to advances in deep network simulation algorithms and design levels and areas of DL architectural style depth efficacy, DL architecture depth has been improved. In contrast to ordinary ANNs, the Modulus is capable of learning modified versions in DL architectures. First and foremost. It is possible to train each layer's features using the output of the preceding layer. Each layer contains a set of features that can be trained on. The most important consideration was how the original photograph would turn out.

In the innermost sphere, more complex qualities are shown to double and multiply. Combine features before layering. A simple user interface makes this possible. A face description model can be built from a vector representation of a portrait's raw image. The input layer is where data from pixels is supplied into a model. It is possible to categorize the first obscured layer (the nose, eyes, etc.) using the edge piece as a characteristic of cream-based lines, which in turn may be used to classify all of the preceding qualities in order to form a face. An example of how each layer can be deciphered from the one before it is shown here. However, empirical development evaluations have shown that DL models perform better than their shallower counterparts for reasons that remain obscure. As far as I'm aware, there isn't any solid proof.

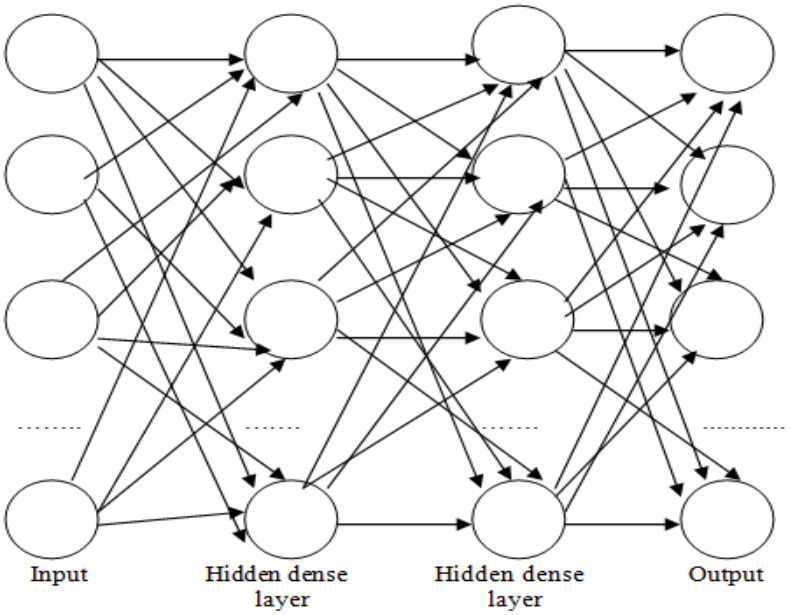

Fig. 3. Deep learning's overall methodology.

4. Method

The proposed systems are shown in Fig. 4 and Fig. 5. Wireless sensor networks are frequently used to measure a variety of physical parameters across a large area (WSN). Large numbers of little nodes make up a Wireless Sensor Network (WSN) (sensors). Environmental variables such as temperature, altitude, humidity, and air quality are collected by these sensors. This is just one of many uses for them, including monitoring natural events such as floods, earthquakes, volcanic eruptions, and other catastrophes. Additionally, they have been used in the fields of robotics, chemistry, and medicine. In the mountains, WSN applications such as altitude, pressure, humidity, and natural disasters are prevalent. It is believed that the foundation of each sensor is a straightforward screen with a limited power supply and memory. In addition, each sensor is thought to include a mechanism for transmitting and receiving data with other nodes as well as a component for determining the characteristics of the area that is being monitored. For almost all WSN applications, it is necessary to be aware of the physical locations of the devices in order for them to work correctly. The information that the sensors collect is useless if you do not know where they are located. In many instances, it is possible to accurately forecast the specific placement of certain nodes. The remainder of the network's design could contain ad-hoc and randomly created Internet of Things devices in order to reduce the amount of bandwidth required to execute the application.

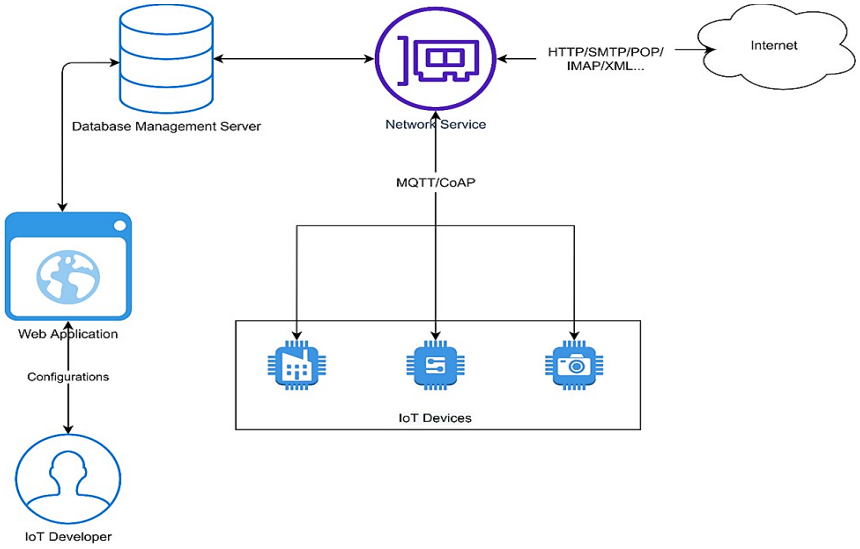

Fig. 4. The suggested system's structure.

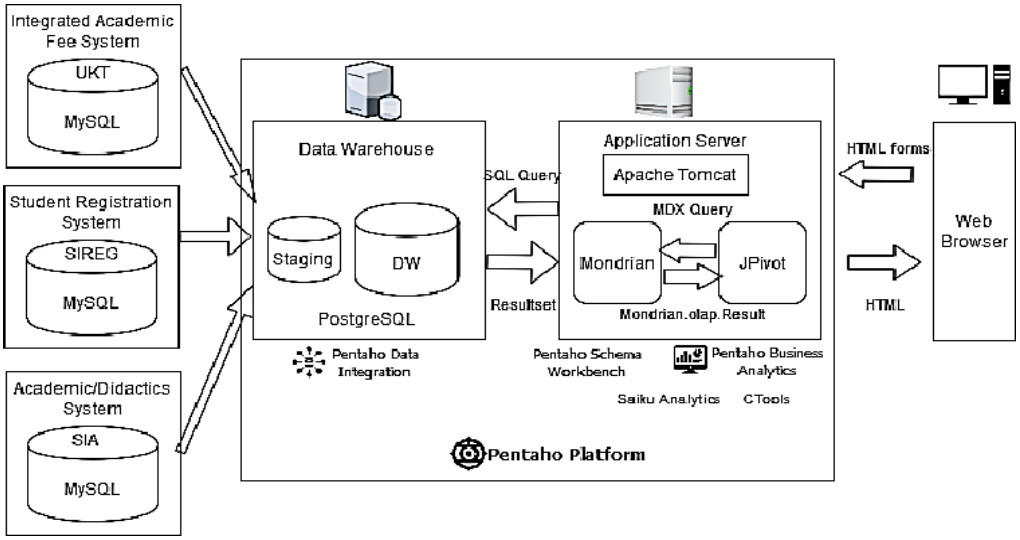

Fig. 5. App forms as they would appear in the final design.

5. Wireless Sensor Network

Sensor-based interactions with the environment set WSNs apart from other types of networks, be they conventional, cable, or even wireless (Fig. 6). Most WSNs have very little or no infrastructure. Sensor nodes range from a few dozen to a few thousand in number. It is possible to monitor and measure a specific area with the help of these sensors. Most of the time, we're looking to make use of low-cost sensors with a small number of processing components. These methods for proxying internet systems in wireless sensor networks are analyzed in this chapter, and their classification and assessment are discussed in the following sections. Based on a variety of factors, they can be categorized into a number of different groups. Because it involves distributed systems, the challenge is framed as such in the thesis. Assumptions are made that a direct link may not be possible over the entire network, as well. This is why hardware limitation is such an important concept to understand.

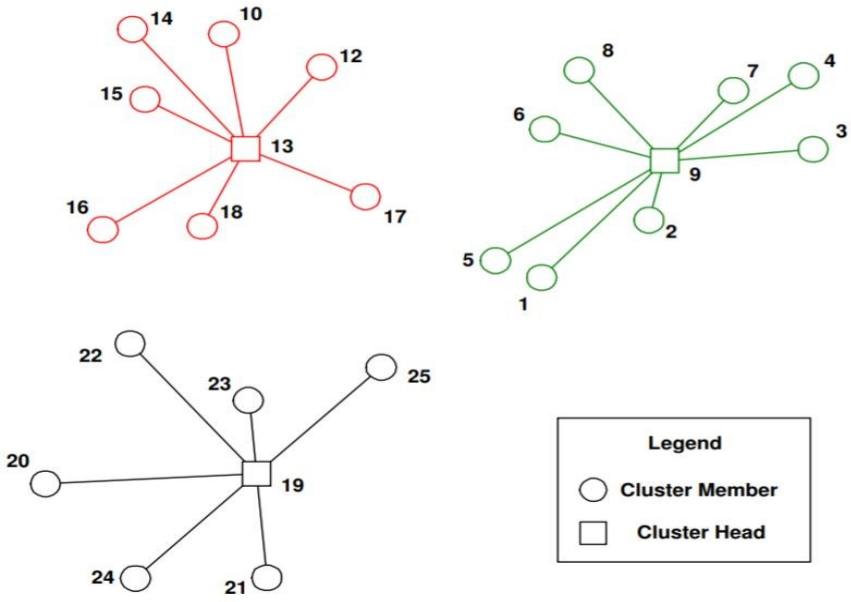

Fig. 6. After clustering wireless sensor networks, the network's topology.

6. Results

Analyzing real-time proxy systems' WSN networks and application data is shown in Fig. 7, Fig. 8, Fig. 9, and Table 1. This is in addition to our comparison and evaluation of WSN clusters with 10-node nodes vs. a prior 2-node clustering technique for application-level information. Additional information was calm from the use layer as well. Despite this, the data was sourced from an open-resource site as well as featured a synthetic dataset. From an extensive collection of wireless sensors and p2p devices, our data has not been synthesized. It was our own software that took the least amount of time to run. Therefore, we decided to investigate the execution times of each method. A review of previous studies indicated the difficulty of handling massive datasets in sensor networks, according to our research. A huge number of calculations can manage a vast dataset with increasingly exact measurements.

Wireless sensor computation has a 98.68 percent accuracy rate and the quickest execution time due to the fact that it operates on a wide variety of categories, but it does not categorize intermediates in real-time; rather, it classifies the "Worms" in a sensor network. The research found that random clusters had a success rate of 99.21% when used for intrusion detection as well as classification on a device system that required practically minimal execution time. First of all, we are able to accurately detect as well as describe real-time proxies types and incursions in sensor-based networks by matching our findings to those of past studies and drawing comparisons between the two sets of data.

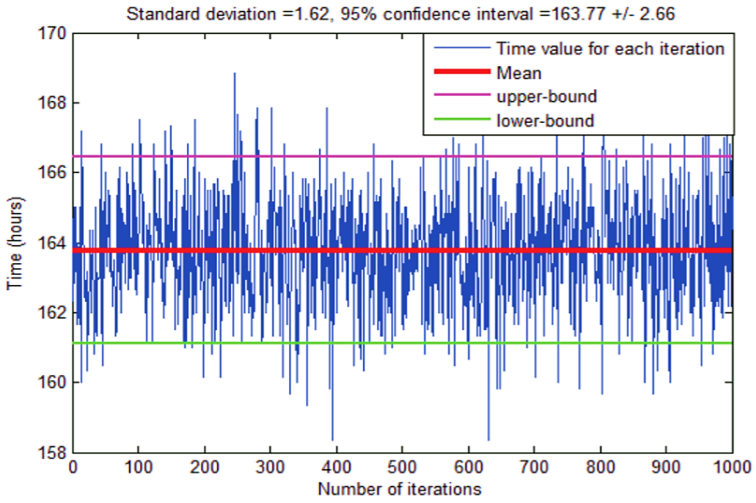

Fig. 7. In order to serve as a proxy for internet traffic, a transportation map of the free time spent in the simulator was created.

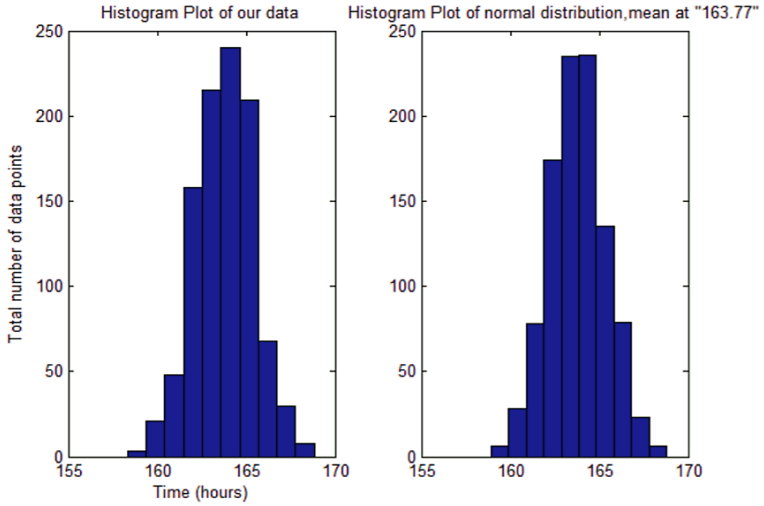

Fig. 8. Histogram depicting the reproduction time relative to the average data point travel time in the WSN.

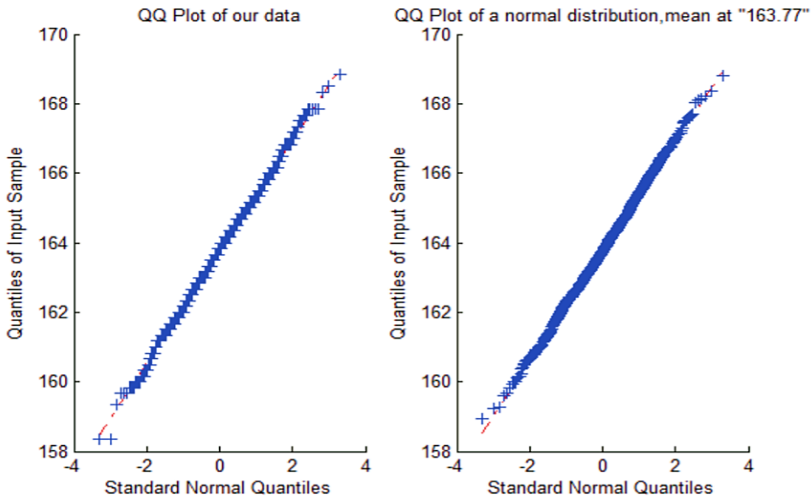

Fig. 9. In contrast to the normal distribution, the simulation represented, over time, quantiles according to the normal standard.

Table 1. The similarity of different methods.

Scientific article	Method	Precision
[32]	S-V-M	89.97 percent
[33]	C-N-N	95.63 percent
Suggested	D-N-N	97.69 percent

7. Conclusion

During the duration of this analysis, no WSN incursions were detected outside of the analyzed clusters and nodes. Create a new column for each original entry in the dataset, and then eliminate the previous columns by substituting them with regression models. This will help you to organize the dataset. A number of 0 in Boolean logic implies that something is false, while a value of 1 implies that a property is true. The decoding of the Tuesday-Working Hours-11/DNS-labeled Results columns. The processing of the.csv file took almost seven hours, whereas the first run of Experiment 1 required 12 hours. To reduce the quantity of data that needed to be examined, the random sample size was reduced from 1 to 0.5. This shows that just fifty percent of the available data is utilized. The next run, in contrast, hand, was ended after eight hours since it did not achieve its aim within a reasonable amount of time. The duration of the study was 29 hours, and the third installment of the process employed only 20% of the obtained data.

8. Future Recommendation

Unit test coverage will be improved, and performance-critical operations will have more benchmarks introduced as part of WSN's future development. It will be checked to see whether any data is missed or misinterpreted by comparing the output of the WSN network with the output of other instruments. Support for extracted features from other scholarly articles is one way that clusters may improve in the future. Experiments with additional datasets should also be conducted to see if WSN can provide the requisite intelligence to accurately forecast network data. As part of the WSN framework, the encoding of feature vectors might be done, which would significantly speed up processing as compared to programming. There will also be a way to add additional request layer encoders that would stream refabrication to the system.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, “Intrusion prevention framework for secure routing in wsn-based mobile internet of things,” *IEEE Access*, vol. 7, pp. 185496–185505, 2019, https://doi.org/10.1109/ACCESS.2019.2960633.

[2] O. B. Mora-Sánchez, E. López-Neri, E. J. Cedillo-Elias, E. Aceves-Martínez, and V. M. Larios, “Validation of IoT infrastructure for the construction of smart cities solutions on living lab platform,” *IEEE Transactions on Engineering Management*, vol. 68, no. 3, pp. 899-908, 2021, https://doi.org/10.1109/TEM.2020.3002250.

[3] M. Murad, O. Bayat, and H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IoT technology," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no.1, pp. 546-557, 2021, https://doi.org/10.11591/ijeecs.v21.i1.pp546-557.

[4] H. M. Marhoon, M. I. Mahdi, E. D. Hussein, and A. R. Ibrahim, "Designing and implementing applications of smart home appliances," *Modern Applied Science*, vol. 12, no. 12, pp. 8-17, 2018, https://doi.org/10.5539/mas.v12n12p8.

[5] M. Shobana and S. Poonkuzhali, "A novel approach to detect IoT malware by system calls using deep learning techniques," *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*, pp. 1–5, 2020, https://doi.org/10.1109/ICITIIT49094.2020.9071531.

[6] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1251-1275, 2020, https://doi.org/10.1109/COMST.2020.2964534.

[7] S. Yao, Y. Zhao, A. Zhang, S. Hu, H. Shao, C. Zhang, L. Su, and T. Abdelzaher, "Deep learning for the internet of things," *Computer*, vol. 51, no. 5, pp. 32–41, 2018, https://doi.org/10.1109/MC.2018.2381131.

[8] Y. Choi, M. El-Khamy, and J. Lee, "Universal deep neural network compression," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 4, pp. 715-726, 2020, https://doi.org/10.1109/JSTSP.2020.2975903.

[9] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Networking Letters*, vol. 1, no. 2, pp. 68–71, 2019, https://doi.org/10.1109/LNET.2019.2901792.

[10] W. Lee, M. Kim, and D.-H. Cho, "Deep cooperative sensing: Cooperative spectrum sensing based on convolutional neural networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 3005–3009, 2019, https://doi.org/10.1109/TVT.2019.2891291.

[11] A. Singh, S. Rathkanthiwar, and S. Kakde, "Leach based-energy efficient routing protocol for wireless sensor networks," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 4654–4658, 2016, https://doi.org/10.1109/ICEEOT.2016.7755602.

[12] M. M. Rashid and N. A. S. Al-Jamali, "Modified w-leach protocol in wireless sensor network," *Journal of Engineering*, vol. 25, no. 3, pp. 68–80, 2019, https://doi.org/10.31026/j.eng.2019.03.06.

[13] J. Guo, C.-K. Wen, S. Jin, and G. Y. Li, "Convolutional neural network based multiple-rate compressive sensing for massive mimo CSI feedback: Design, simulation, and analysis," *IEEE Transactions on Wireless Communications*, vol. 19, no. 4, pp. 2827-2840, 2020, https://doi.org/10.1109/TWC.2020.2968430.

[14] A. Mukherjee, P. Goswami, L. Yang, S. K. S. Tyagi, U. C. Samal, and S. K. Mohapatra, "Deep neural network-based clustering technique for secure IIOT," *Neural Computing and Applications*, vol. 32, no. 20, pp. 16109–16117, 2020, https://doi.org/10.1007/s00521-020-04763-4.

[15] L. Mou, L. Bruzzone, and X. X. Zhu, "Learning spectral-spatial-temporal features via a recurrent convolutional neural network for change detection in multispectral imagery," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 57, no. 2, pp. 924–935, 2019, https://doi.org/10.1109/TGRS.2018.2863224.

[16] A. Sonny, P. K. Rai, A. Kumar, and M. Z. A. Khan, "Deep learning-based smart parking solution using channel state information in lte-based cellular networks," *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 642–645, 2020, https://doi.org/10.1109/COMSNETS48256.2020.9027447.

[17] A. Belmonte-Hernández, G. Hernández-Peñaloza, D. M. Gutiérrez, and F. Álvarez, "Recurrent model for wireless indoor tracking and positioning recovering using generative networks," *IEEE Sensors Journal*, vol. 20, no. 6, pp. 3356-3365, 2019, https://doi.org/10.1109/JSEN.2019.2958201.

[18] R. Yang, L. Feng, H. Wang, J. Yao, and S. Luo, "Parallel recurrent convolutional neural networks-based music genre classification method for mobile devices," *IEEE Access*, vol. 8, pp. 19629–19637, 2020, https://doi.org/10.1109/ACCESS.2020.2968170.

[19] X. Zhang, Y. Dong, L. Wen, F. Lu, and W. Li, "Remaining useful life estimation based on a new convolutional and recurrent neural network," *2019 IEEE 15th International Conference on Automation Science and Engineering (CASE)*, pp. 317–322, 2019, https://doi.org/10.1109/COASE.2019.8843078.

[20] M. Farsi, M. Badawy, M. Moustafa, H. A. Ali, and Y. Abdulazeem, "A congestion-aware clustering and routing (CCR) protocol for mitigating congestion in wsn," *IEEE Access*, vol. 7, pp. 105402–105419, 2019, https://doi.org/10.1109/ACCESS.2019.2932951.

[21] A. Mukherjee, D. K. Jain, P. Goswami, Q. Xin, L. Yang, and J. J. Rodrigues, "Back propagation neural network based cluster head identification in mimo sensor networks for Intelligent Transportation Systems," *IEEE Access*, vol. 8, pp. 28524-28532, 2020, https://doi.org/10.1109/ACCESS.2020.2971969.

[22] S. Balakrishna, M. Thirumaran, V. K. Solanki, "IoT sensor data integration in healthcare using semantics and machine learning approaches," *A handbook of internet of things in biomedical and cyber physical system*, pp. 275–300, 2020, https://doi.org/10.1007/978-3-030-23983-1_11.

[23] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," *IEEE Network*, vol. 33, no. 5, pp. 27–33, 2019, https://doi.org/10.1109/MNET.001.1800503.

[24] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, "Adversarial examples–security threats to covid-19 deep learning systems in medical IoT devices," *IEEE Internet of Things Journal*, vol. 8, no 12, pp. 9603-9610, 2021, https://doi.org/10.1109/JIOT.2020.3013710.

[25] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, "An IoT-cloud based wearable ECG monitoring system for smart healthcare," *Journal of medical systems*, vol. 40, no. 12, 2016, https://doi.org/10.1007/s10916-016-0644-9.

[26] W.-J. Hu, J. Fan, Y.-X. Du, B.-S. Li, N. Xiong, and E. Bekkering, "Mdfc–resnet: An agricultural IoT system to accurately recognize crop diseases," *IEEE Access*, vol. 8, pp. 115287–115298, 2020, https://doi.org/10.1109/ACCESS.2020.3001237.

[27] L. Zhou, Z. Qiu, and Y. He, "Application of WeChat mini-program and wi-fi soc in agricultural IoT: A low-cost greenhouse monitoring system," *Transactions of the ASABE*, vol. 63, no. 2, pp. 325–337, 2020, https://doi.org/10.13031/trans.13499.

[28] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, 2019, https://doi.org/10.3390/fi11040094.

[29] D. Rahbari and M. Nickray, "Low-latency and energy-efficient scheduling in fog-based IoT applications," *Turkish Journal of Electrical Engineering Computer Sciences*, vol. 27, no. 2, pp. 1406–1427, 2019, https://doi.org/10.3906/elk-1810-47.

[30] H. Nasiri, S. Nasehi, and M. Goudarzi, "Evaluation of distributed stream processing frameworks for IoT applications in smart cities," *Journal of Big Data*, vol. 6, no. 1, 2019, https://doi.org/10.1186/s40537-019-0215-2.

[31] M.-D. Gonzalez-Zamar, E. Abad-Segura, E. Vazquez-Cano, and E. Lopez- Meneses, "IoT technology applications-based smart cities: Research analysis," *Electronics*, vol. 9, no. 8, p. 1246, 2020, https://doi.org/10.3390/electronics9081246.

[32] B. Zhang, W. Hu, D. Cao, Q. Huang, Z. Chen, and F. Blaabjerg, "Deep reinforcement learning–based approach for optimizing energy conversion in integrated electrical and heating system with renewable energy," *Energy Convers. Manag*, vol. 202, p. 112199, 2019, https://doi.org/10.1016/j.enconman.2019.112199.

[33] H. Guangjie, W. Shen, T. Q. Duong, M. Guizani, and T. Hara, "A proposed security scheme against Denial of service attacks in cluster-based wireless sensor networks," *Security Comm. Networks*, vol. 7, pp. 2542– 2554, 2014, https://doi.org/10.1002/sec.373.