YIDDISH Vol 10 Issue 02,June 2020
ISSN NO: 0364-4308

The use of a Neural Network Algorithm for 5G Network Simulation in a Smart City Environment

DR.DODLA PRATHYUSHA REDDY[1], SADA MADHURI[2],
PROFESSOR[1], ASSISTANT PROFESSOR[2],
DEPARTMENT OF ECE
PBR VISVODAYA INSTITUTE OF TECHNOLOGY AND SCIENCE::KAVALI

Abstract:

The introduction of 4G technology has led to a notable increase in internet speed, and the introduction of 5G technology promises an even faster transmission rate with coverage both inside and outdoors in smart cities. That 5G is on the horizon raises the possibility that Wi-Fi may be superseded by it for use in applications like geo-location that need constant radio coverage, so ushering in the widespread deployment of the Internet of Things. Although the introduction of Wi-Fi 6 would benefit IoT applications, 5G will be required for smart cities to make advantage of Big Data in internet service provision, thereby reducing the requirement for mobile networks and supplementary private network equipment. Nonetheless, as network access continues to grow, the threat of cyber security grows along with it. More digital targets will become available to thieves when mobile and wireless networks share access channel architecture. To address these issues, we have presented a blockchain-based random neural network that may be used in a variety of contexts to improve online safety. Here, neural weights are used to encode the data while protecting the privacy of the user. However, data mining of the victim's compromised identity may often reveal the attacker. A safe and decentralised authentication system is proposed in this work. These results confirm that adding a random neural network to a blockchain improves the efficiency, usability, and security of the network.

keywords

Smart cities, 5G, IoT, Blockchain, and a Random Neural Network are some examples

Introduction

In recent years, "smart cities" have become the norm as their inhabitants become more reliant on them. The features of a standard smart city should be built to be accessible at all times. Despite the fact that technical progress has allowed for a wide variety of human-machine, machine-to-machine, and human-to-human combinations in terms of applications and services, novel and inventive means of supplying energy to smart cities have yet to be identified. A smart city is based on the internet of things, which allows for the processing and interchange of large amounts of data, the deployment of servers and sensors, and the integration of an extensive network of devices. It is possible to detect physical values, and it is possible to detect virtual information; both can be converted to digital form, which may then be coupled with a transmitter and delivered across a wired or wireless network [1]. Improvements in communication protocols, transmission networks, decentralisation, edge computing, and the cloud are all technologies that have contributed to the emergence of the Internet of Things. The Internet of Things has opened up a variety of possibilities for enhanced services and more thoughtful policymaking in the context of smart cities. The broad use of IoT has led to advancements in asset management, energy efficiency, and maintenance expenses, among other areas. Since massive MIMO antennas, device densities, extreme node density, incredible bandwidth, and high carrier frequency are required in smart cities, 5G will prove to be a game-changing technology best adapted to these circumstances. Some potential applications of 5G include vast M2M communications, ultra-reliable low-latency communications [2,] and enhanced mobile broadband.

Connecting 5G's air interface and spectrum with Wi-Fi and LTE will make it a highly integrative technology, opening the door for global connectivity solutions that are inexpensive, accessible, scalable, reliable, and user-friendly [3]. These capabilities of 5G are what are driving the internet forward towards the creation of smart cities. Enhanced Quality of Service, reduced latency, and high data throughput are just a few of the supplementary characteristics needed for deployment in smart cities. Increasing the intelligence and flexibility of 5G is necessary to enhance the capacity of the node, as well as the cost and energy efficiency of the network as a whole. Residents in "smart cities" are given access to Big Data and the Internet of Things in order to assist them make more informed decisions. The Internet of Things (IoT) will continue to play a critical role in enabling the construction of trustworthy systems for monitoring, managing, and controlling these devices; for storing and analysing large volumes of data; and for integrating essential insights into Smart City Users [4]. Information prediction in mobile phones, energy efficiency, proactive maintenance, and asset maintenance are only few of the problems that become significantly less complicated when big data is applied.

Connected Pieces

Numerous new smart city apps have been released, all of which make use of blockchain technology to bolster the existing security infrastructure of connected gadgets. In this first stage, actuators and sensors in a physical layer send and collect data, which is then passed on to the protocol layer below. Transmission techniques such as Bluetooth, Ethernet, 5G, and 4G are all conceivable in the communications layers that may use blockchain protocols to increase data privacy and security [5, 6]. The data from the physical layer is stored in a distributed ledger in the database layer. One may classify this data as private, public, permissioned, or unrestricted. This interface layer is used by many different smart apps, such as those concerned with health, the house, and parking, all of which work together to make informed choices. A blockchain-based intelligent transportation system may be built up in many tiers as well [7]. Services and applications that deal with packaging, such as logistics and ridesharing, are part of the application layer. Smart contracts, algorithms, and scripts that can enforce themselves and carry out their own execution and verification make up the contract layer. This layer is made operational by the static data stored on the blockchain. The incentive layer integrates the blockchains with the monetary reward, outlining the procedures for distribution and issuing.

The consensus layer's agreement method encompasses the proof-of-work, proof-of-stake, and proof-of-movement layers. In the networking layer, tasks including authentication, data forwarding, and peer-to-peer communication are performed through a distributed network of peers. The solution's physical layer consists of the various field assets, while the data layer displays the linked data blocks [8]. The same holds true for other Blockchain analytical tools like Merkle trees, hash methods, time stamping, and asymmetric encryption. Multiple industries and groups will benefit from 5G, including cloud providers and tenants, infrastructure, mobile network operators, and others. When independent IoT devices are linked together through 5G networks or the internet, it poses a range of cyber security risks that might compromise private data [9]. In order to provide self-network management, data analytics, and decentralised applications, mobile-edge computing and fog computing will be essential as 5G adoption rises [10]. As a result of these cyber security concerns in 5G networks, deep learning methods are proposed to help identify and investigate network abnormalities. It is normal practise to use a mobile cloud computing based wireless network that employs 5G to counteract threats in the Intrusion Detection system and Web security sector [11, 12].

Proposed Work

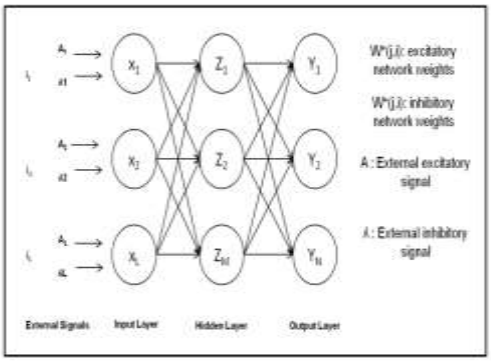

A_1
a_1
A_2
a_2
A_L
a_L
X_1
X_2
X_L
Z_1
Z_2
Z_M
Y_1
Y_2
Y_N
W⁺(j,i): excitatory network weights
W⁻(j,i): inhibitory network weights
A : External excitatory signal
λ : External inhibitory signal
External Signals
Input Layer
Hidden Layer
Output Layer

Fig.1. Structure of a Random Neural Network

Blockchain relies on cryptographic ideas that may also be applied with Neural networks. In the blockchain, large amounts of data are organised into blocks that include metadata such as a date, a hash of the preceding block, and the number of times the block has been mined. The hash is computed by the distributed miners to verify the current block. Details of transactions validated with the help of the smart city's final destination, the transaction's point of origin, and a private key will be stored in a blockchain inside the smart city's data. As can be seen in Fig.1, a Random Neural Network is constructed using a stochastic model spiked in a recurrent mode. This method is used to monitor transmissions of signals in the formusing a biological neural network but communicating only via spikes (instead of analogue signals) [13]. n neurons make up a Random Neural Network [14], and the equation below represents the state of each neuron in that network at a given time t.

$$k(t) = [k_1(t), k_2(t), \dots\dots\dots, k_i(t)] \qquad (1)$$

where $ki\ (t)$ denotes the neuron potential in a given time t. Using the spikes in terms of amplitude, the neurons communicate with each other. The following are the representation of the different spikes transmitted:

- When a negative spike occurs, it is detected as an inhibition signal which causes a fall of the neuron potential by one unit, $kn\ (t\ +) = km(t) - 1$

- When a positive spike occurs, it is detected as an excitation signal and will cause the neuron potential to increase by a unit, $kn\ (t\ +) = km(t) + 1$ where where the receiving neural is m and $km(0)$ will have no effect.

- If the potential is positive, the neurons will accumulate signals and use it to fire. This process will occur in a random fashion and the spikes that are fired at this instance will have a rate r(i) and are independent in inter-spike intervals, distributed in an exponential fashion.

Radom Neural Network Model

A random neural network will comprise of the following parts namely Decentralized information, Neural Chain Network, Validation and Data and Private key. The private key is represented as Y which is made up of application or user digital credentials that are assigned to a particular user. This will comprise of biometrics and will require encryption with a proper algorithm like 256-cipher Advanced Encryption Standard (AES). The private key can be denoted as $Y = (y1,\ y2,\ \dots\ \dots\ ,\ yN)$ and can be updated with new data as and when necessary, using validation of user credentials. $V(t) = (V1, V2,\ \dots\ \dots\ ,\ VN)$ is used to validate the data, $D = (d1,\ d2,\ \dots\ \dots\ ,\ dN)$ using I-vectors where $no = (i1,\ i2,\ \dots\ \dots\ ,\ iI)$ where the dimensions are denoted using I. For an input state $X = xI$, the first validation $V1$ can be identified and user data is defined as$d1$. The value of neural chain can be denoted as the hidden layer $Z = zM$ and the user private key can be used in $Y = yN$which can be inserted during the next transaction at the input layer. Using a decentralized network, the calculated neural network weights $w\ -(x,\ y)$ and $w\ +(x,\ y)$ are saved and can be recovered during mining process. Similarly the next validation $V2$ is connected to $X = xI$, the input state which is related to the hidden layer ZM , the chain and $d1$ of the first validation $V1$, along with additional data $d2$. The value of neural chain for the upcoming transaction is identified using the hidden layer $Z = zN$ and the user private key using the output state$Y = yN$. As the data inserted increases, the process also iterates. Based on selection of neurons, the values associated with the hidden layer neurons and a combination of stored neural weights from the private key, the neural chain can be formulated. Using neural network weights $w\ -(x,\ y)$ and $w\ +(x,\ y)$ in Random neural network output determination, data can be mined or validated, at random inputs of$X = xI$. Hence this process will also be similar to that of traditional blockchain where the hash tag has to be found by the miners. When the input is discovered, such that the output Y can be decoded with an error lesser than a predefined limit that can be used for recovering the weights, mining of random neural network with block chain configuration takes place. The error Ek can be expressed as:

$$E_k = \frac{1}{2}\sum_{n=1}^{N}(y'_n - y_n)^2 < T$$

where yn denotes the secret code, X = xI the random input, and y ′ n the neural network's random output, and Ek the minimal error value. Modifying the parameter Ek allows us to control the level of difficulty encountered when mining. Following the discovery of the optimal solution, the user or application's data will be processed. In a similar vein, the user's new data will be added to the previous values, as well as a possible hidden layer value Z = zN, to form a neural chain that will serve as the input for the following transaction. After the weights of the neural network are set at w (x, y) and w +(x, y), the gradient descent learning process is employed to determine the random neural network for a new pair. The mining process will scale proportionally with the growing user base. The user data is encrypted using the weights w (x, y) and w +(x, y) and then stored as a decentralised network rather than being distributeddirectly. When mining is performed on user data, encryption is utilised to access the data with the use of a biometric key, and the data is then stored in the distributed system. The weights in a neural network grow dynamically as verification data is added.

Results and Discussion

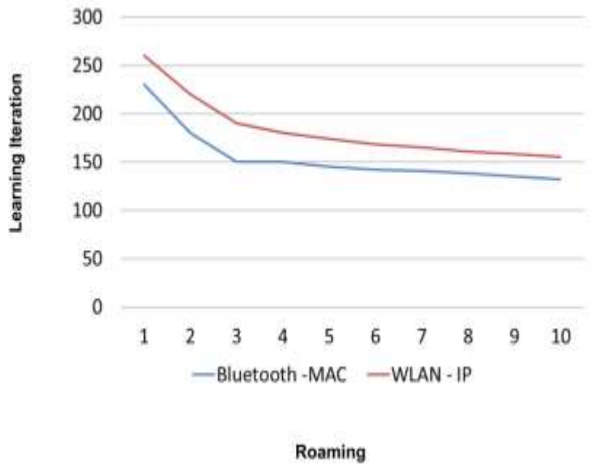
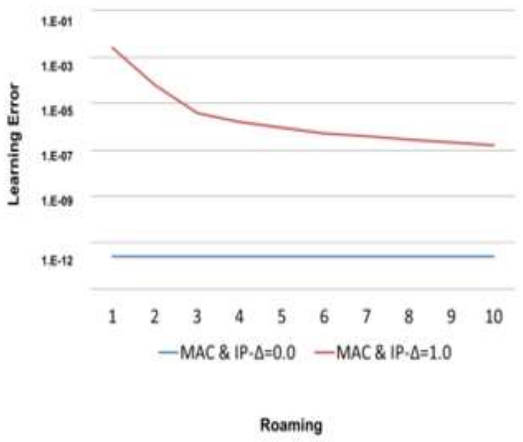


Fig.2. Tampering Error Observed in Bluetooth and WLAN

The impact of manipulation on the neural block chain may be determined with the help of the learning algorithm. By keeping an eye on the variations at a change of =1, the mistake rate may be lowered. In this case, both networks are monitored simultaneously while their values are varied in increments of one. Figure 2 depicts a Bluetooth and WAN simulation used to calculate the tampering error, and Figure 3 displays the divergence between MAC and IP addresses for = 0 and = 1.

Fig.3. Changes in Δ with respect to MAC & IP



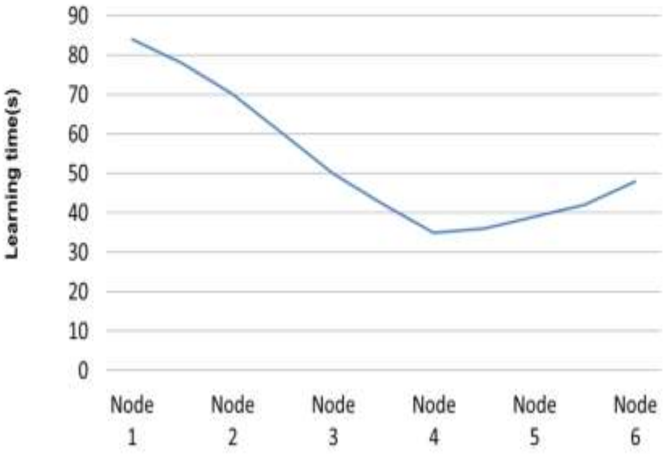


Fig.4 Learning and Mining Iterations in 5G network simulation

The hidden layer holds four neurons with learning progressing in a continuous manner. Fig.4 shows the simulation for 5G nodes activated. It is observed that due to random values uses, the mining iteration is not as expected.

Conclusion

The number of neurons in the aforementioned random neural network used in 5G and the Internet of Things for smart cities increases based on the confirmed user data. Incorporating a 5G node authentication method allowed us to show that progressive mining in a decentralised network with encrypted data is necessary for developing a neural network that supports smart city infrastructure. Malicious users or cybercriminals might be used to verify the accuracy of the findings. Applying the suggested approach to other neural networks to evaluate and compare mining outputs might be useful for future study in this area. Mining's impact may be determined during authentication and roaming by striking a good balance between user data and the number of neurons.

References

[1] Latif, Shahid, Zhuo Zou, Zeba Idrees, and Jawad Ahmad. "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network." IEEE Access 8 (2020): 89337-89350.

[2] Bi, X. A., Jiang, Q., Sun, Q., Shu, Q., & Liu, Y. (2018). Analysis of Alzheimer's disease based on the random neural network cluster in fMRI. Frontiers in neuroinformatics, 12, 60.

[3] Brun, O., Yin, Y., Gelenbe, E., Kadioglu, Y. M., Augusto-Gonzalez, J., & Ramos, M. (2018, February). Deep learning with dense random neural networks for detecting attacks against iot-connected home environments. In International ISCIS Security Workshop (pp. 79-89). Springer, Cham.

[4] Gelenbe, E., & Yin, Y. (2017, October). Deep learning with dense random neural networks. In International Conference on Man–Machine Interactions (pp. 3-18). Springer, Cham.

[5] Bashar, A. (2019). Survey on evolving deep learning neural network architectures. Journal of Artificial Intelligence, 1(02), 73-82.

[6] Pierangeli, D., Palmieri, V., Marcucci, G., Moriconi, C., Perini, G., De Spirito, M., ... & Conti, C. (2018). Deep optical neural network by living tumour brain cells. arXiv preprint arXiv:1812.09311.

[7] Yang, G. (2019). Scaling limits of wide neural networks with weight sharing: Gaussian process behavior, gradient independence, and neural tangent kernel derivation. arXiv preprint arXiv:1902.04760.

[8] Benali, L., Notton, G., Fouilloy, A., Voyant, C., & Dizene, R. (2019). Solar radiation forecasting using artificial neural network and random forest methods: Application to normal beam, horizontal diffuse and global components. Renewable energy, 132, 871- 884.

[9] Kong, Y., & Yu, T. (2018). A deep neural network model using random forest to extract feature representation for gene expression data classification. Scientific reports, 8(1), 1-9.

[10] Vijayakumar, T. (2019). Comparative study of capsule neural network in various applications. Journal of Artificial Intelligence, 1(01), 19-27.

[11] Muneera, B. H., Janeera, D. A., Shankar, B. M., & Anita, S. D. R. (2020, September). Edge Preserving Filter Selection for Noise Removal and Histogram Equalization. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 567-571). IEEE.

[12] Liu, Y., Zhong, Y., Fei, F., Zhu, Q., & Qin, Q. (2018). Scene classification based on a deep random-scale stretched convolutional neural network. Remote Sensing, 10(3), 444.

[13] Raj, J. S., & Ananthi, J. V. (2019). Recurrent neural networks and nonlinear prediction in support vector machines. Journal of Soft Computing Paradigm (JSCP), 1(01), 33-40.

[14] Katuwal, R., & Suganthan, P. N. (2019). Stacked autoencoder based deep random vector functional link neural network for classification. Applied Soft Computing, 85, 105854.