Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

5G Network Simulation in Smart Cities using Neural Network Algorithm

Dr. S. Smys,
Professor, Department of Computer Science and Engineering,
RVS Technical Campus,
Coimbatore, India.
Email: smys375@gmail.com

Dr. Haoxiang Wang,
Department of Electrical and Computer Engineering, Cornell University,
Ithaca, USA.
Email: wanghaoxiang1102@hotmail.com

Dr. Abul Basar,
Professor,
Prince Mohammad Bin Fahd University,
Kingdom of Saudi Arabia.
Email: abashar@pmu.edu.sa

Abstract: The speed of internet has increased dramatically with the introduction of 4G and 5G promises an even greater transmission rate with coverage outdoors and indoors in smart cities. This indicates that the introduction of 5G might result in replacing the Wi-Fi that is being currently used for applications such as geo-location using continuous radio coverage there by initiating the involvement of IoT in all devices that are used. The introduction of Wi-Fi 6 is already underway for applications that work with IoT, smart city applications will still require 5G to provide internet services using Big Data to reduce the requirement of mobile networks and additional private network infrastructure. However, as the network access begins to expand, it also introduces the risk of cyber security with the enhanced connectivity in the networking. Additional digital targets will be given to the cyber attackers and independent services will also be sharing access channel infrastructure between mobile and wireless network. In order to address these issues, we have introduced a random neural network blockchain technology that can be used to strengthen cybersecurity in many applications. Here the identity of the user is maintained as a secret while the information is codified using neural weights. However, when a cyber security breach occurs, the attacker will be easily tracked by mining the confidential identity. Thus a reliable and decentralized

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

means of authentication method is proposed in this work. The results thus obtained are validated and shows that the introduction of the random neural network using blockchain improves connectivity, decentralized user access and cyber security resilience.

Keywords: Smart cities, 5G, Internet of Things, Blockchain, Random Neural Network.

1. Introduction

Smart Cities have become a general norm of usage as their implementation in the society increases to meet the different user requirements and needs. The functionality of a typical smart city should be such that they are always ready to be used. Though the development in technology has facilitated many human to machine, machine to machine and human to human combinations in terms of applications and services, unique smart city drivers are yet to be invented. The internet of things forms the backbone of a smart city, with big data processing and exchange, servers and sensors and interconnected system of devices. In IoT, the physical values can be sensed while virtual information can be detected and converted to a digital form such that can be integrated with a transmitter to travel over a wireless or wired medium of network communication [1]. The evolution of communication protocols, transmission networks, decentralization, edge computing and cloud computing has resulted in the introduction of IoT. The implementation of IoT in smart cities has opened the gateway to an array of applications for higher level services and intelligent decision making. This introduction of IoT has resulted in a number of advantages such as maintenance, energy usage and assets. Hence 5G will prove to be a novel solution apt for smart cities that require large MIMO antennas, device densities, extreme node density, great bandwidth and high carrier frequency.

Some of the areas in which 5G finds its applications are massive machine type communications, ultra reliable low latency communications [2] and enhanced mobile broadband. Moreover, 5G will also prove to be very integrative by connecting the spectrum and air interface of 5G with Wi-Fi and LTE, enabling cost-efficient, easily-available, scalable, reliable and global connectivity solutions providing seamless user experience and high coverage [3]. These characteristics of 5G have driven the internet towards expanding into smart cities. However, when using in smart cities, there are some extra features that need to be involved such as an improvement in the Quality of Service, low latency and high data

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

rate. Intelligence and flexibility of the 5G needs to be increased to improve capacity of the node and further improve cost and energy efficiency. The use of Big Data with IoT in smart cities will ensure that the citizens make informed decisions with data correlations and data analytics. As the number of smart devices that we are using increases steadily, IoT remains the key source of enabling proper management and establishment of monitoring, managing and controlling the smart devices, keeping track of and analyzing large volumes of data using big data and incorporating key insights into Smart City Users [4]. A number of problems related to information prediction in mobile phone, energy optimization, proactive maintenance and asset maintenance becomes easier when Big data is involved.

2. Related Works

A number of applications have introduced for smart city uses blockchain technology to improve the security framework in smart devices. This introduction is through the use of actuators and sensors in a physical layer to transmit data and gather data to be sent to the next protocol layer. Bluetooth, Ethernet, 5G and 4G are the different data transmission methods that are possible in the communications layers where it is possible to incorporate blockchain protocols, to enhance privacy and security of the data [5-6]. A distributed ledger is present in the database layer which is used to save the information from the physical layer. This information can be classed as either private, or public and permissioned or permission-less. There are many smart applications for this interface layer like smart health, smart home and smart parking, integrated with one another to formulate sound decisions. Many layers can also be used to establish an intelligent transport system working on the basis of blockchain [7]. The application layer encompasses the packaging services and applications like logistics and ride sharing. The contract layer is built with smart contracts, algorithms and scripts that are self-enforcing, self-executing and self-verifying. The static data that is saved in the blockchain is used to activate this layer. The incentive layer incorporates the block chains with the economic reward such that allocation methods and issuance are specified. The proof of movement, proof of stake and proof of work come under the agreement algorithm in the consensus layer. Distributed peer-to-peer verification, data forwarding and networking are involved in the network layer. The data layer shows the chained data blocks while the physical layer comprises of the different field assets of the solution [8]. Similarly, it will also include Merkle trees, hash algorithms, time stamping, asymmetric encryption techniques that

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

are used in Blockchain analysis. 5G will find its place in a number of applications such as cloud service providers and tenants, infrastructure, mobile network operators and various other stakeholders. The interconnection of standalone IoT systems using the 5G networks or internet will lead to a number of cyber security challenges, resulting in exposure of sensitive information [9]. As the use of 5G increases, mobile-edge computing and fog computing will play a crucial role in self network management, data analytics and decentralized applications [10]. Hence deep learning techniques are introduced as a solution for cyber security issues in 5G to trace network anomalies. In Intrusion Detection system and Web security domain, a mobile cloud computing based wireless network that uses 5G to mitigate threats are commonly implemented [11-12].

3. Proposed Work

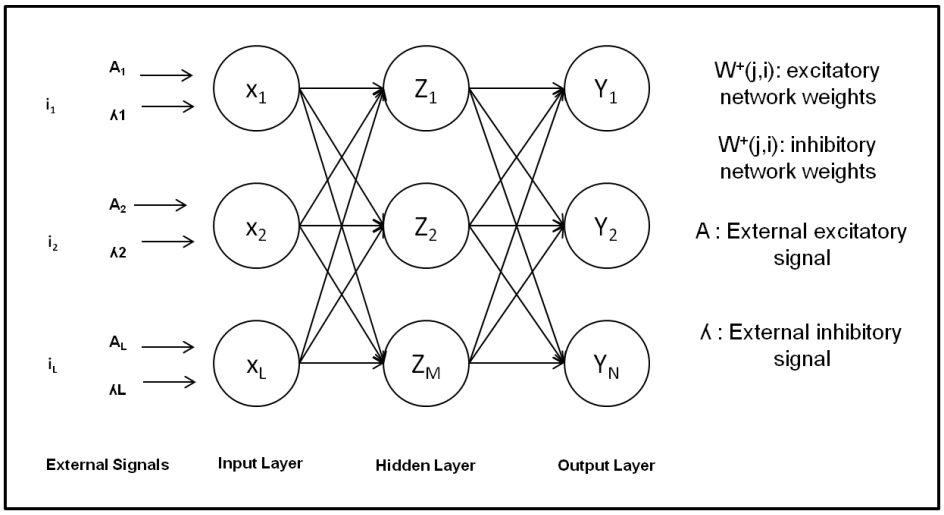

Fig.1. Structure of a Random Neural Network

Cryptographic concepts form the basis for blockchain and can also be used with Neural networks. The Big data or information is stored in the blockchain in forms of blocks with parameters like previous block hash, count of attempts to mine the block and timestamp. To validate the current block, the hash is calculated using the decentralized miners. The blockchain in the smart city information will hold details of the transaction that are authenticated with the aid of smart city destination, transaction origin and private key. A Random Neural Network is built with a stochastic model that is spiked in a recurrent mode as shown in Fig.1. This approach is used to observe the signals that are transmitted in the form

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

of spikes instead of analog signals, through biological neural network [13]. A Random Neural network [14] is made up of n-neurons and each network of the neuron at a particular time 't' can be denoted as the equation below:

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

where $k_i(t)$ 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, $k_n(t^+) = k_m(t) - 1$
- When a positive spike occurs, it is detected as an excitation signal and will cause the neuron potential to increase by a unit, $k_n(t^+) = k_m(t) + 1$ where where the receiving neural is m and $k_m(0)$ 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.

3.1 Random 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 $Y = (y_1, y_2, \dots\dots, y_N)$ and can be updated with new data as and when necessary, using validation of user credentials. $V(t) = (V_1, V_2, \dots\dots, V_N)$ is used to validate the data, $D = (d_1, d_2, \dots\dots, d_N)$ using I-vectors where $n_o = (i_1, i_2, \dots\dots, i_I)$ where the dimensions are denoted using I. For an input state $X = x_I$, the first validation V_1 can be identified and user data is defined asd_1. The value of neural chain can be denoted as the

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

hidden layer $Z = z_M$ and the user private key can be used in $Y = y_N$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 V_2 is connected to $X = x_I$, the input state which is related to the hidden layer Z_M, the chain and $d_1$of the first validation V_1, along with additional data d_2. The value of neural chain for the upcoming transaction is identified using the hidden layer $Z = z_N$ and the user private key using the output state$Y = y_N$. 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$X = x_I$. 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 E_k can be expressed as:

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

where y_n is the private key or application or user, $X = x_I$ is the random input and y'_n is the random neural network output, E_k is the threshold or minimum error value. On adjusting the value of E_k we can tune the mining complexity. When the final solution is mined or found, the data of application or user will be processed. Similarly $Z = z_N$ which will be a potential neural hidden layer value will be added to the existing values to develop a neural chain which will act as the next transaction's input, in addition to the user new data. As the last step, gradient descent learning algorithm is used to determine the random neural network for a new pair with weights of the neural network fixed to be $w^-(x,y)$ and$w^+(x,y)$. As the number of new users increases, the mining process will also increase simultaneously.

Rather than distributing the data directly, the user data is first encrypted using the weights $w^-(x,y)$ and $w^+(x,y)$ which are saved as a decentralized network. Decryption of the data is used inside the mining process is done on the user data with the help of a biometric key

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

thereby saving the information in the decentralised system. As the data to be verified is inserted, the neural network weights expand by in an adaptable manner.

4. Results and Discussion

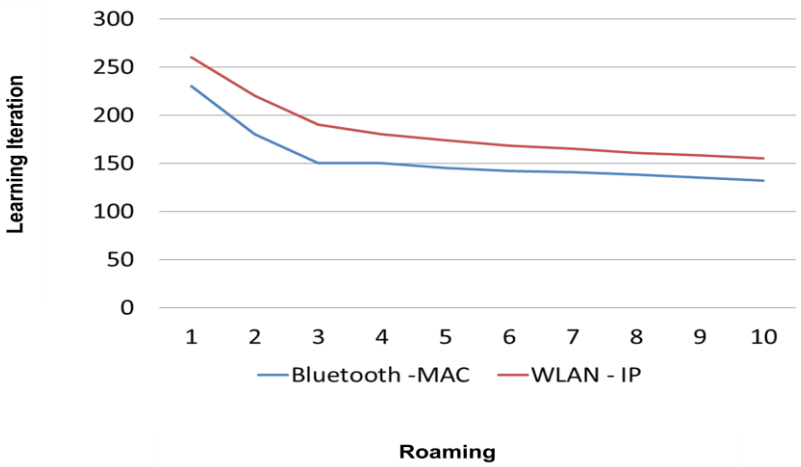

Fig.2. Tampering Error Observed in Bluetooth and WLAN

Using the learning algorithm, we can find the tampering effect on the neural block chain. It will reduced the rate of error, by observing the differences at a change of Δ=1. Here both the networks are observed at the same phase using varying values in steps of unity. Fig.2 shows the Bluetooth and WAN simulation for determining the tampering error while Fig.3 indicates the difference in MAC & IP for value of 0 and 1 for Δ.

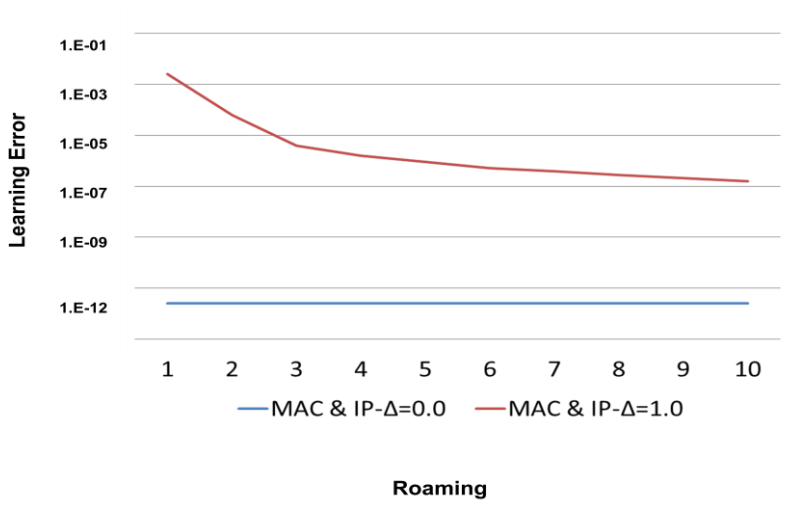

Fig.3. Changes in Δ with respect to MAC & IP

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

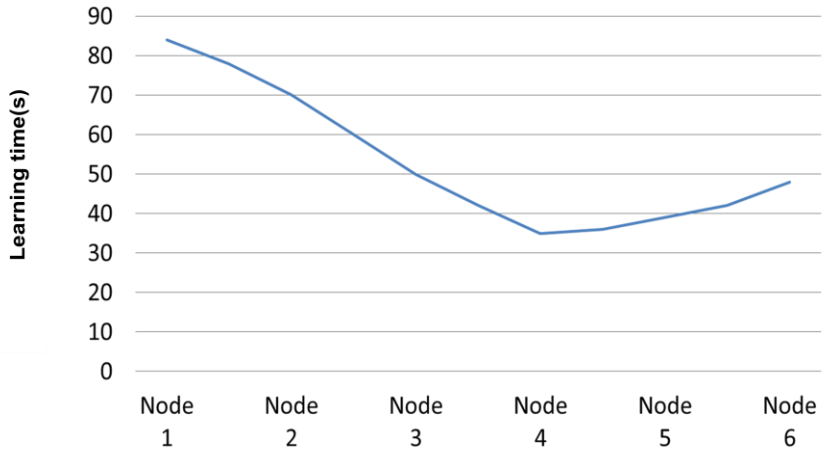

Fig.4 Learning and Mining Iterations in 5G network simulation

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.

5. Conclusion

The proposed work is the implementation of random neural network in 5G and IoT for smart cities where as the data validation of the users increases, the neurons will also gradually increase. A 5G node authentication process is incorporated and the observed results indicated that in order to aptly build a neural network that supports smart city infrastructure, mining should take place in a gradual manner in a decentralized network with encrypted data. Moreover, results can also be validated using cyber attackers or rogue users can be identified and detected. Future research in this methodology could include using the proposed methodology in other neural networks in order to compare and contrast the results of mining. The authentication stages and Roaming stages will be able to determine the mining effect and a proper balance needs to be struck between the user data as well as 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.

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

[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.

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.01
Pages: 43-52
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.1.004

[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.

ISSN: 2582-2012 (online)
Submitted: 21.01.2021
Revised: 25.02.2021
Accepted: 15.03.2021
Published: 29.03.2021