HIGHLY SECURE AND ACCURATE DEEP SLICING IN 5G WIRELESS NETWORKS FOR EFFICIENT RESOURCE UTILIZATION

Ambidi Naveena

Electronics and Telematics Engineering Department, G. Narayanamma Institute of Technology and Science (for women), Shaikpet, Hyderabad, Telangana, India

E-mail of corresponding author: naveenaambidi@gmail.com

Ambidi Naveena 0000-0002-0691-9494

Resume

Both the current cellular network and the planned 5G mobile network need to meet high dependability standards, very low latency requirements, larger capacity, better security and fast user communication. In order to support multiple independent tenants on the same physical infrastructure, mobile carriers are working towards end-to-end network resource allocation in 5G networks. Future communication networks will require data-driven decision making due to the increase in traffic and the accelerated performance of 5G networks. With the use of in-network deep learning and prediction, a "deep slice" model was built in this study to control network load efficiency and network availability. Even in the event of a network outage, the suggested model is capable of making wise selections and choosing the best network slice.

Article info

Received 16 August 2022
Accepted 1 February 2023
Online 24 April 2023

Keywords:

cellular communications
CNN
prediction
network slicing
deep slicing

Available online: https://doi.org/10.26552/com.C.2023.042

ISSN 1335-4205 (print version)
ISSN 2585-7878 (online version)

1 Introduction

The International Telecommunication Union (ITU) published a paper in February 2017 that outlined important requirements, including baseline standards for the technical performance for IMT-2020 for 5G mobile communication technology. The minimum bandwidth need for next-generation services is 1 GHz, the maximum data transfer rate is 20 Gbps and the smallest latency time is 1 ms. These are the basic needs for a variety of 5G services as well as the technological requirements to achieve the three main goals of 5G: ultra-fast, super-connection and ultra-low latency. Compared to 4G mobile communication, 5G mobile communication is more innovatively improved in terms of speed, employing protocol and network setups [1].

Twenty times quicker than current long-term evolution (LTE), the 5G wireless network is designed as a soft defined network (SDN), while the 5G core network has been switched from a centralized to a decentralized kind to reduce traffic transmission latency. Development of ubiquitous, digital services with anytime, everywhere connection will rely heavily on 5G networks. A wide range of applications, from ubiquitous internet access to driverless cars, will be made possible by them. The present COVID-19 pandemic age appears to have confirmed the value and significance of communication networks and related services [2].

With the advent of Beyond 5G systems, which offer cutting-edge services like holographic communications, Virtual Reality (VR), this function is anticipated to become even more important for implementation of a future digital society. An “IoT communication environment” may be realized by offering a quicker “mobile communication environment,” when the capacity and speed of data transmission and reception across the wired and wireless networks is equal. Such an ecosystem can deliver realistic media content in 4K, VR and 8K, while also ensuring low power consumption in Internet of Things devices and service reliability even in settings with many connected devices, thanks to cutting-edge technology like AR, VR, drones and smartphones [3].

The ITU-R divided the three main 5G mobile network services into three categories: ultrahigh speed and big capacity (Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (uRLLC) and Massive Machine-Type Communications (mMTC)), depending on the needs of each service in terms of bandwidth, speed and latency. The technology aspires to deliver up to 20 times the speed, 10 times the number of connections to IoT devices and 10 times the number of low-latency services, compared to 4G mobile communication technology. In addition to undertaking an examination of LTE security threats, the European Union Agency for Cyber security (ENISA) divided 5G network threat types into seven categories. It then used the CIA criteria to examine them as a threat landscape. Through the use of the 5G threat surface, 5G America in the USA classified the possible security risks [4].

The biggest challenge for 5G is the sheer volume of networked devices, including vital infrastructure that must be utilized in a brand-new IoT paradigm with unequal resources. To achieve the desired functionality, challenges must be overcome, including protection against DoS attacks on end-user devices, protection against DoS attacks on radio interfaces, devices and networks, distributed control systems that require coordination to prevent Signal storms and protection against DoS attacks on infrastructure. Additionally, similar issues are highlighted by Next Generation Mobile Networks (NGMN) [5].

The remaining portions of this article are structured as follows: The existing work is presented in Section 2. Section 3 present the proposed deep slicing in 5G wireless networks. The result analysis is presented in the section 4. Section 5 concludes the work.

2 Literature survey

Park et al. proposed the potential security risks that could exist in the 5G NSA network, they were examined, validated on the live network and recommendations for security improvements were made. In addition, authors examined the necessity for the new security strategies rather than conventional security methods and associated research and demonstrated the persistent weaknesses in the current mobile network system. 5G mobile communication network backgrounds and historical data collected to match with current situation to detect the threats in real-world mobile networks in service. Before releasing the new services, it is vital to assess the potential security risks they may pose as well as appropriate mitigation strategies. [6].

Ortiz et al. developed INSPIRE-5Gplus1 project, which is creating a smart, reliable and responsible 5G security platform. This platform utilizes cutting-edge methods for closed-loop and end-to-end security management in 5G and Beyond 5G networks, including Distributed Ledger Technologies (DLT), Machine Learning (ML), Artificial Intelligence (AI), Trusted Execution Environment (TEE) and Network Softwarization. Security management with Security Service Level Agreements (SSLAs) and liability management are the key aspects of INSPIRE-5Gplus1 platform. [7].

Suomalainen et al. proposed the most significant issue that arises from the direct use of ML ideas in the 5G network infrastructure, which is weakened network security. In addition to providing potential vulnerabilities and attack pathways against the availability and integrity of 5G services, ML enables user surveillance and privacy violation assaults that were previously unattainable with conventional adversarial tactics. This work's primary goal was to promote further study into the secure application of ML methods in 5G and other future wireless networks [8].

Waziri et al. proposed an enhanced reference monitor algorithm for the Software Defined Networking (SDN) controller for 5G security. Over 50 billion connections are anticipated, which the present 4G network cannot support. While ubiquitous mobile broadband is the primary goal of 4G networks, 5G technological characteristics will need to significantly improve. Software's adaptability is essential for fulfilling unanticipated future service requirements. In this context, Software Defined Networking (SDN) has lately gained traction in the networking sector, albeit a precise standard on how to assess security risks on SDN for 5G has not yet been implemented. To implement the access control policy, this paper suggests using the 5-ENSURE architecture to integrate Reference Monitor (RM) with SDN controllers. The Study will also isolate and handle malicious packets in a distributed manner among nodes rather than only permitting or denying access based on access policy [9].

More than 50 billion connections are anticipated as a result, more than 4G can manage at this time. While ubiquitous mobile broadband is the primary focus of 4G networks, 5G technology requirements must significantly outpace those. To accommodate the unanticipated future service need, software flexibility is essential. In this context, Software Defined Networking (SDN) has just recently gained traction in the networking sector and a clear standard has not yet been set on how to assess the security risks on SDN for 5G. This study suggests using the 5-ENSURE architecture and combining Reference Monitor (RM) with SDN controllers to apply access control policies. [10].

Sciancalepore et al. proposed the development of three crucial network slicing building elements that are in charge of (i) traffic analysis and prediction per network slice, (ii) admission control choices for network slice requests and (iii) adaptive load forecast correction based on measured deviations. These findings demonstrate a trade-off between cautious forecasting setups and more aggressive ones, as well as extremely significant potential advantages in terms of system usage [11].

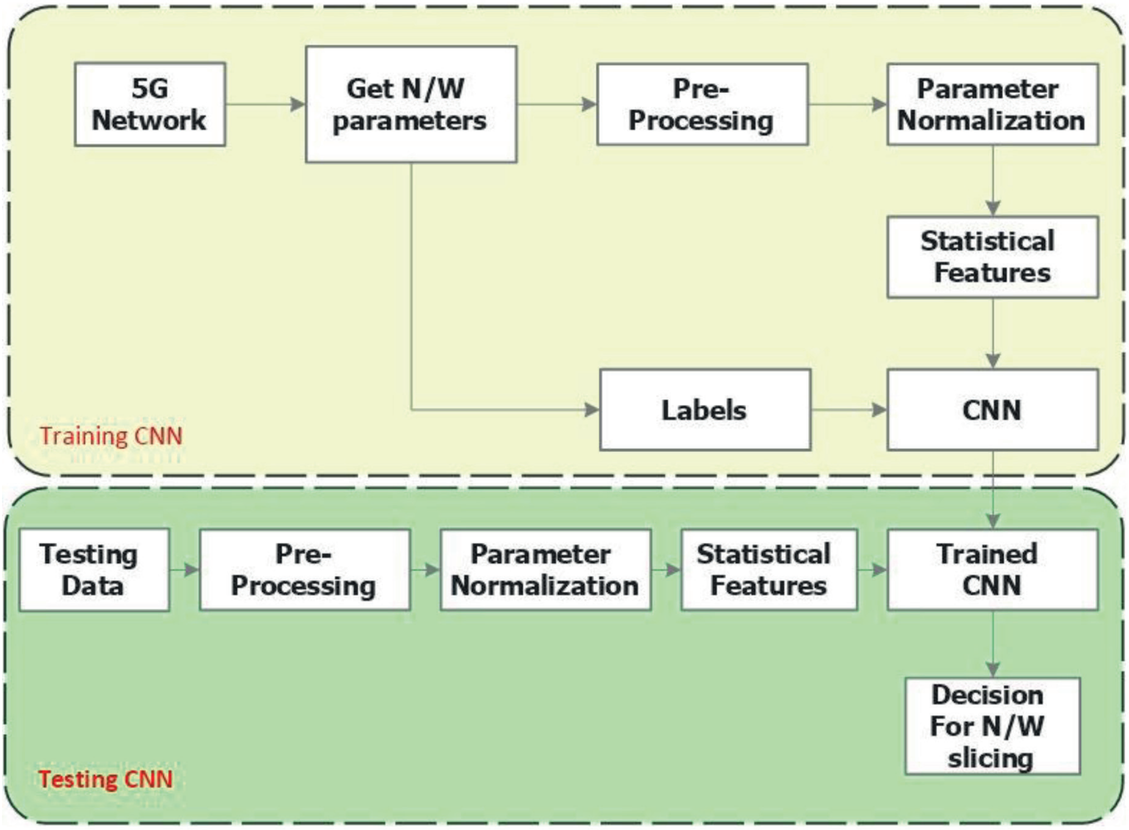

Figure 1 *Block diagram of the proposed method*

Feng et al. proposed a wireless network virtualization paradigm including the data plane, cognitive plane and control plane as its three components. To support the suggested concept, a unique control signaling method has been developed, as well. A hierarchical control method, based on the cell-clustering, has been employed with dynamically optimized resource consumption from the standpoint of network virtualization. To show how the schemes operate under the suggested paradigm to enhance resource efficiency and the user experience, two cases of application have been examined [12].

The main objectives of the proposed methods are

- Create a productive technique to improve the system's overall effectiveness in terms of system throughput and energy efficiency.
- The interference in 5G networks and IoT systems is reduced or eliminated.

3 Proposed method

The risks and security issues the 5G ecosystem faces are largely the same as those that 4G/LTE users are now dealing with. To achieve the service level agreements for a variety of applications and services, 5G networks will also have unique requirements on throughput, latency and security, especially with a diversified ecosystem for the IoT devices [13]. Utilize the 5G network to obtain network parameter, employing the FoG computing for preprocessing. After a parameter has been normalized, apply statistical characteristics. Apply CNN network for categorization at the end.

3.1 Block diagram

Efficient resource utilization in 5G networks can improve the quality of the service in terms of connectivity, speed and quality etc. Frequency slicing can improve the resources' utilization in networks. The proposed block diagram for resources' utilization using slicing with CNN is shown in Figure 1. Initially, the network parameters are extracted to perform the resource utilization process. All the collected parameters are normalized using min max level to perform highly accurate feature extraction process. Statistical features are extracted to feed the CNN for training and classification further.

3.2 Preprocessing

3.2.1 Fog computing

Fog nodes in 5G are situated at the radio access network's edge (RANs). Researchers from Cisco characterized fog computing as "a platform that provides compute, communication and data storage capabilities between end devices and standard cloud computing platforms." Although many issues have been solved by integrating cloud computing and end devices, the concentration of resources in cloud computing creates a significant disconnect between the IoT devices and the cloud [13-14]. The resulting massive communication latency and computing overhead will surely rise.

3.3 Parameter normalization

Data must be standardized in order to get the best results while learning the deep learning network parameters. The subsequent equation is applied to each feature in this work's data normalization, using the min-Max method [15]. The general equation, used to perform the normalization process is given as:

$$normalization = \frac{y - y_{\min}}{y_{\max} - y_{\min}}, \tag{1}$$

where y defines the data to be normalized, y_{min} is the value of minimum, y_{max} is the value of maximum.

3.4 Statistical features

Network characteristics gathered include the protocol's packet size, the number of packets per flow, different payload patterns, the size of the payload and the protocol's request time distribution [16]. Initial raw packet captures are transformed to network flows for simpler analysis in order to identify the characteristics from these profiles. The first packet defines the forward (source to destination) and backward (destination to source) directions for bidirectional flows created with CICFlowMeter. Therefore, they are estimated independently both for forward and backward directions, using the 83 statistical data acquired from the flows, such as time, number of packets, number of bytes and packet length.

3.4.1 Arithmetic features

Standard Deviation: The standard deviation in statistics is a metric for the variation of the distribution of a collection of data. The formula for the sample standard deviation is:

$$\sigma = \sqrt{\frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})^2}, \tag{2}$$

where x_n are the observed values, $\bar{x}$ is the mean value, N is the number of observations.

Mean: By adding up all of the numerical values of the observations and dividing the result by the total number of observations, the mean of a set of observed data can be calculated. It is given in Equation (3).

$$\bar{x} = \frac{1}{n} \quad \left(\sum_{i=1}^{n} x_i\right) = \frac{x_1 \ + x_2 \ + \cdots \ + x_n}{n}. \tag{3}$$

Kurtosis: Kurtosis is a statistical metric used to assess how "tailed" a real-valued random variable's probability distribution, given by:

$$\text{Kurtosis}[X] = E\left[\left(\frac{X-\mu}{\sigma}\right)^4\right] = \frac{E\left[(X-\mu)^4\right]}{\left(E\left[(X-\mu)^2\right]\right)^2} = \frac{\mu_4}{\sigma^4}, \tag{4}$$

where μ_4 is the fourth central moment and σ is the standard deviation. K denotes the kurtosis.

Skewness: In probability theory and statistics, skewness is a measure of the asymmetry of the probability distribution of a real-valued random variable in regard to its mean.

The skewness of a random variable X is the third standardized moment $\tilde{\mu}_3$ defined as:

$$\tilde{\mu}_3 = E\left[\left(\frac{X-\mu}{\sigma}\right)^3\right] = \frac{\mu_3}{\sigma^3} = \frac{E\left[(X-\mu)^3\right]}{\left(E\left[(X-\mu)^2\right]\right)3/2} = \frac{k_3}{k_2^{3/2}}, \tag{5}$$

where μ represents the mean, σ represents the standard deviation, E represents the expectation operator, μ_3 is the third central moment and κ_t is the t-th cumulants.

3.5 CNN

Three factors make the CNN's structure: dataset quantity, quality and type. The many receptive layers can process elements of the input layer. These networks may be set up such that an output picture with a high resolution may be produced by creating an overlap of the input region. Convolutional neural networks (CNNs) are used for feature detection. Following feature extraction, a classifier is created using all the fully linked layers. Convolutional layers and pooling layers couple less frequently since a fully linked CNN is not required. It is regarded as CNN's beating centre [17]. Convolution is used when the two mathematical functions are combined, with the outcome also being a function. By moving the filter, convolution is carried out over the input. The result of matrix multiplication for each place is added to the feature map, as a total [18]. The input picture for this layer is s*s*p, where s is the image's height and width and p is a channel with many filters, each of which is t*t*q in size. The picture dimension is lower than t and q can be the same as channel s [19].

Pooling Layer: between the CNN and the convolution layer, there is an inclusion of a pooling layer. The major objective of this layer is to reduce the dimensionality to get minimal computation and fewer parameters. Max pooling is the most significant pooling. It is employed to select the highest value available in each window [20-23].

Fully Connected Layer: The Fully Connected

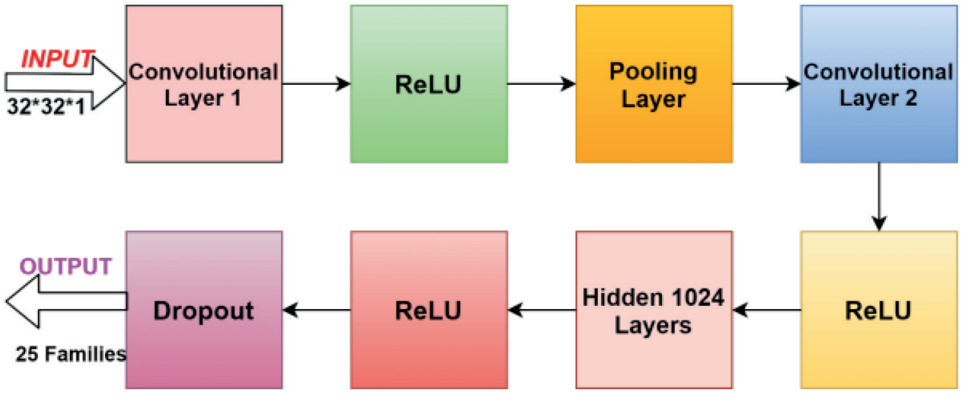

Figure 2 *Architecture of CNN*

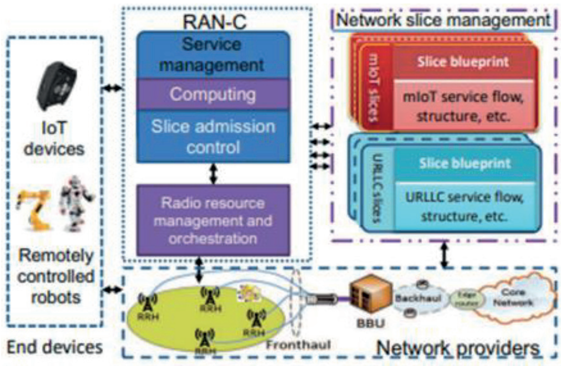

Figure 3 *Systematic diagram of RAN Slicing*

Layer, which classifies input pictures as a last layer after convolutional and pooling, is used. Having neurons that are linked to the preceding layer performs activation activities in a layer that is completely connected. It will also offer information security to identify and categorize bad code in addition to malware detection. Figure 2 depicts the structure of CNN.

3.6 RAN slicing

Slicing the radio access network (RAN) is a key idea for effectively distributing the current network infrastructure across several vertical applications. Running numerous logical or virtual networks as distinct business activities on a single RAN is characterized as RAN slicing. Every network slice is a separate logical network that has been designed to meet the quality-of-service (QoS) requirements of a certain application. Additionally, various sophisticated radio access technologies (RATs), including massive MIMO, coordinated multi-point (CoMP) transmission and full-duplex need to be investigated in order to meet the hard connectivity requirements. One of the most important RATs that satisfies the rigid reliability criterion for tactile applications is coMP transmission, which generates spatial variety with redundant communication channels. The division of a RAN using the CoMP transmission mechanism (referred to as a CoMP-enabled RAN) into many virtual networks is the definition of the idea of CoMP-enabled RAN slicing. The systematic diagram of RAN Slicing is shown in Figure 3.

4 Results and discussions

4.1 Dataset

uses the deep learning to achieve effective and dependable network slicing in 5G networks. It contains the day and time of each linking, which may also assist the network forecast of the amount of connections at any particular moment in the future and it would be knowledgeable of which networking slices will be obligatory or demanded by those links, based on information gathered from the previous data.

4.2 False positive rate

The percentage of negative test results that regardless result in positive test results is known as the false positive rate; it is the conditional probability of a positive test result given the absence of a specific event. The significance level is matched by the false positive rate. One less than the false positive rate is the test's specificity.

4.3 Positive predictive value

The positive and negative predictive values are the proportions of occurrences in statistical and screening procedures that are really positive and genuinely negative findings (PPV and NPV, respectively). The effectiveness of a diagnostic test or other statistical metric is described by the PPV and NPV. The correctness of such a statistic can be inferred from a high result. As opposed to true positive and true negative rates, which are inherent to the test, the PPV and NPV also depend on the prevalence of the test. The equations for PPV and NPV are given in Equations (6) and (7), respectively.

$$PPV = \frac{No.of\ TP}{No.of\ TP + No.FP}, \tag{6}$$

$$NPV = \frac{No.of\ TN}{No.of\ TN + No.FN}. \tag{7}$$

Throughput: It is a gauge of how quickly a node can send data across a network. Throughput, then, is the typical rate of successfully delivering messages through a communication connection.

Packet Delivery Ratio: the proportion of packets successfully received by the destination node to those successfully sent by the source node. The packet delivery ratio is given as:

$$Packet\ Delivery\ Ratio = \frac{Total\ number\ of\ packets\ received}{Total\ number\ of\ packets\ send}. \tag{8}$$

Highlights of the DeepSlice simulation model's

***Table 1** Highlights of DeepSlice's simulation model's features*

Input type	Packet Loss Rate	Packet Delay Budget (ms)	Normalized Duration (s)
Smart phone	10^{-2}	60	257
IoT devices	10^{-2}	50	54
Smart transportation	10^{-6}	10	52
AR / VR / Gaming	10^{-3}	50	534
Smart City / Home	10^{-2}	10	100
Unknown Device Type	10^{-6}	10	60

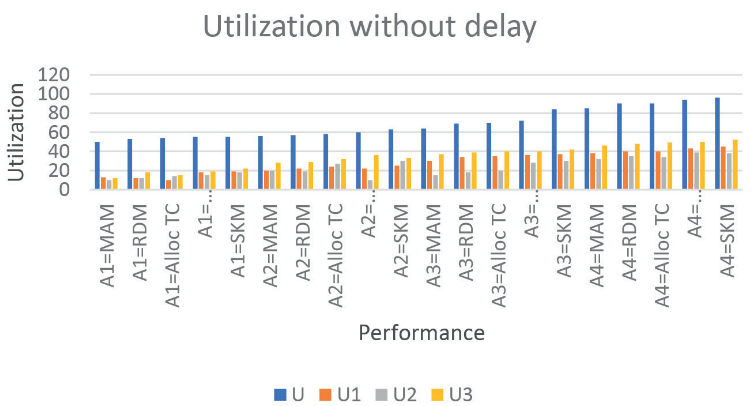

***Figure 4** Performance of utilization without delay*

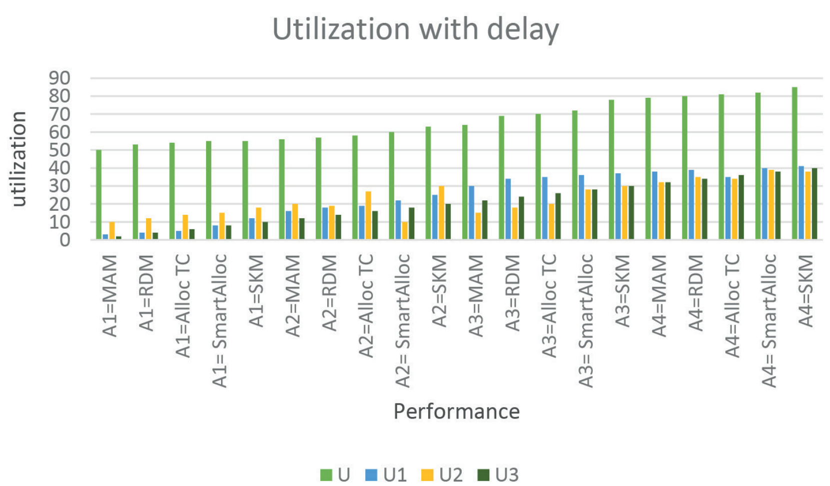

***Figure 5** Performance of utilization with delay*

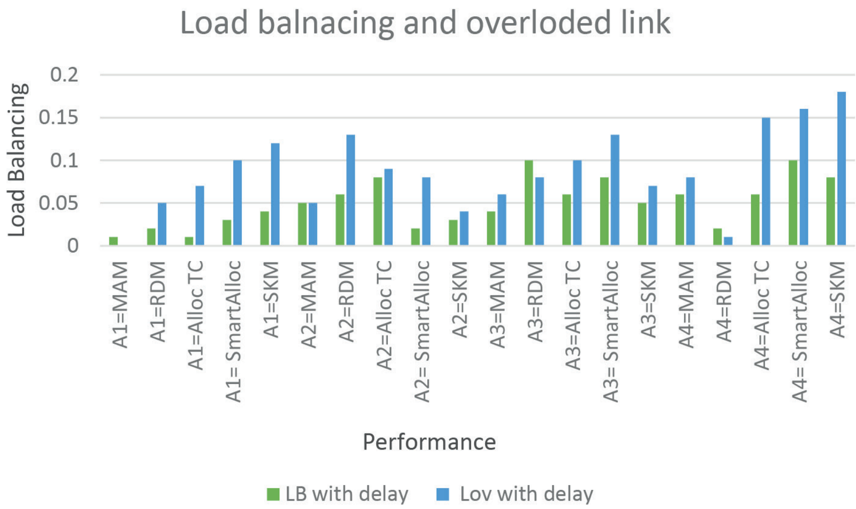

Figure 6 *Performance of load balancing with delay*

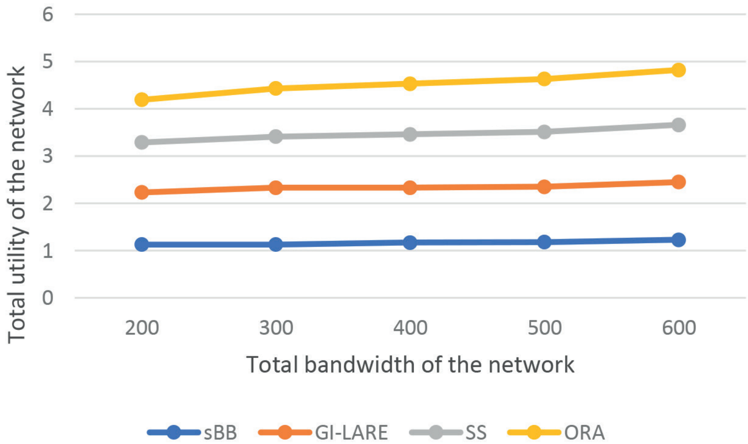

Figure 7 *Impact of the total bandwidth on the total utility of the network at 10 ms delay bound*

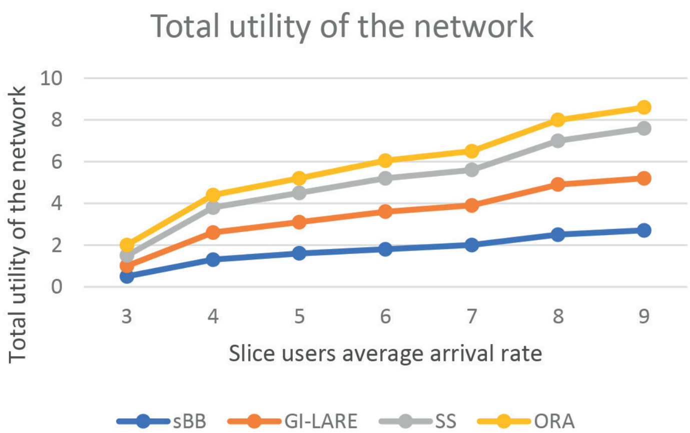

Figure 8 *Effect of the slice user density on the total utility of the network*

characteristics are listed in Table 1. As expected, each of these inbound requests is routed to one or more of the network slices. The first responders in an emergency may use smartphones to make phone calls, access the internet and send the text messages, all at once.

Figure 4 shows the performance of utilization without delay. Figure 5 depicts the performance of utilization with delay. Figure 6 displays the performance of load balancing with delay. Figure 7 depicts the effect of network utility on total bandwidth at a 10 ms delay bound. The impact of slice user density on the overall network utility is seen in Figure 8.

5 Conclusions

To support the connecting of IoT devices, the 5G network adopted a software-defined architecture, bringing technological advantages. In this work, the 5G parameters from the 5G network were obtained and preprocessed using the Fog computing methodologies. Then the preprocessing parameter are normalized. Then, the feature is extracted using the statistical features, like standard deviation, mean, kurtosis, skewness from the normalized parameter. Finally, the CNN is trained by using extracted arithmetic features to perform highly accurate packet slicing process. While the 5G Security is a step forward, the vulnerabilities associated with interconnecting with the older networks against a considerably higher volume of data and applications continue to increase. When compared to other previous works, the CNN-based RAN slicing approach used in this work delivers the high efficiency and secure data of the 5G network.

Grants and funding

The author received no financial support for the research, authorship and/or publication of this article.

Conflicts of interest

The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] BHARDWAJ, A. 5G for military communications. *Procedia Computer Science* [online]. 2020, **171**, p. 2665-2674. eISSN 1877-0509. Available from: https://doi.org/10.1016/j.procs.2020.04.289

[2] YESMIN, T., AGASTI, S., CHAKRABARTI, K. 5G security and privacy issues: a perspective view. In: *ICT with intelligent applications. Smart innovation, systems and technologies* [online]. SENJYU, T., MAHALLE, P.N., PERUMAL, T., JOSHI, A. (Eds.). Vol. 248. Singapore: Springer, 2022. ISBN 978-981-16-4176-3, eISBN 978-981-16-4177-0, p. 89-98. Available from: https://doi.org/10.1007/978-981-16-4177-0_12

[3] DANGI, R., JADHAV, A., CHOUDHARY, G., DRAGONI, N., MISHRA, M. K., LALWANI, P. ML-Based 5G network slicing security: a comprehensive survey. *Future Internet* [online]. 2022, **14**(4), 116. eISSN 1999-5903. Available from: https://doi.org/10.3390/fi14040116

[4] SHI, W., XU, W., YOU, X., ZHAO, CH., WEI, K. Intelligent reflection enabling technologies for integrated and green internet-of-everything beyond 5G: communication, sensing and security. *IEEE Wireless Communications* [online]. 2022, Early Access, p. 1-8. ISSN 1536-1284, eISSN 1558-0687. Available from: https://doi.org/10.1109/MWC.018.2100717

[5] KIM, H. 5G core network security issues and attack classification from network protocol perspective. *Journal of Internet Services and Information Security (JISIS)* [online]. 2020, **10**(2), p. 1-15. ISSN 2182-2069, eISSN 2182-2077. Available from: https://doi.org/10.22667/JISIS.2020.05.31.001

[6] PARK, S., KIM, D., PARK, Y., CHO, H., KIM, D., KWON, S. 5G security threat assessment in real networks. *Sensors* [online]. 2021, **21**(16), 5524. eISSN 1424-8220. Available from: https://doi.org/10.3390/s21165524

[7] ORTIZ, J., SANCHEZ-IBORRA, R., BERNABE, J. B., SKARMETA, A., BENZAID, CH., TALEB, T., ALEMANY, P., MUNOZ, R., VILALTA, R., GABER, CH., WARY, J.-P., AYED, D., BISSON, P., CHRISTOPOULOU, M., XILOURIS, G., MONTES DE OCA, E., GUR, G., SANTINELLI, G., LEFEBVRE, V., PASTOR, A., LOPEZ, D. INSPIRE-5Gplus: intelligent security and pervasive trust for 5G and beyond networks. In: 15th International Conference on Availability, Reliability and Security: proceedings [online]. 2020. ISBN 978-1-4503-8833-7, p. 1-10. Available from: https://doi.org/10.1145/3407023.3409219

[8] SUOMALAINEN, J., JUHOLA, A., SHAHABUDDIN, S., MAMMELA, A., AHMAD, I. Machine learning threatens 5G security. *IEEE Access* [online]. 2020, **8**, p. 190822-190842. eISSN 2169-3536. Available from: https://doi.org/10.1109/ACCESS.2020.3031966

[9] WAZIRI, J. U., OMOKHUALE, E. Development of enhance reference monitor algorithm for software defined networking (SDN) controller for 5G security. *International Journal of Multidisciplinary Research and Growth Evaluation* [online]. 2022, **3**(3), p. 226-241. eISSN 2582-7138. Available from: https://doi.org/10.54660/anfo.2022.3.3.15

[10] PRADHAN, D., SAHU, P. K., GOJE, N. S., GHONGE, M. M., TUN, H. M., RAJESWARI, R., PRAMANIK, S. Security, privacy, risk and safety toward 5G green network (5G-GN). In: *Cyber security and network security* [online]. PRAMANIK, S., SAMANTA, D., VINAY, M., GUHA, A. (Eds.). Scrivener Publishing LLC, 2022. ISBN 9781119812494, eISBN 9781119812555, p. 193-216. Available from: https://doi.org/10.1002/9781119812555.ch9

[11] SCIANCALEPORE, V., SAMDANIS, K., COSTA-PEREZ, X., BEGA, D., GRAMAGLIA, M., BANCHS, A. Mobile traffic forecasting for maximizing 5G network slicing resource utilization. In: IEEE Conference on Computer Communications INFOCOM 2017: proceedings [online]. IEEE. 2017. ISBN 978-1-5090-5337-7, eISBN 978-1-5090-5336-0, p. 1-9. Available from: https://doi.org/10.1109/INFOCOM.2017.8057230
[12] FENG, Z., QIU, CH., FENG, Z., WEI, Z., LI, W., ZHANG, P. An effective approach to 5G: wireless network virtualization. *IEEE Communications Magazine* [online]. 2015, **53**(12), p. 53-59. ISSN 0163-6804, eISSN 1558-1896. Available from: https://doi.org/10.1109/MCOM.2015.7355585
[13] EL-MEKKAWI, A., HESSELBACH, X., PINEY, J. R. Evaluating the impact of delay constraints in network services for intelligent network slicing based on SKM model. *Journal of Communications and Networks* [online]. 2021, **23**(4), p. 281-298. ISSN 1229-2370, eISSN 1976-5541. Available from: https://doi.org/10.23919/JCN.2021.000024
[14] OLADEJO, S. O., FALOWO, O. E. Latency-aware dynamic resource allocation scheme for multi-tier 5G network: a network slicing-multitenancy scenario. *IEEE Access* [online]. 2020, **8**, p. 74834-74852. eISSN 2169-3536. Available from: https://doi.org/10.1109/ACCESS.2020.2988710
[15] SHAHRIAR, N., TAEB, S., CHOWDHURY, S. R., ZULFIQAR, M., TORNATORE, M., BOUTABA, R., MITRA, J., HEMMATI, M. Reliable slicing of 5G transport networks with bandwidth squeezing and multi-path provisioning. *IEEE Transactions on Network and Service Management* [online]. 2020, **17**(3), p. 1418-1431. eISSN 1932-4537. Available from: https://doi.org/10.1109/TNSM.2020.2992442
[16] RAMRAO, J. V., JAIN, A. Dynamic 5G network slicing. *International Journal of Advanced Trends in Computer Science and Engineering* [online]. 2021, **10**(2). ISSN 2278-3091. Available from: https://doi.org/10.30534/ijatcse/2021/741022021
[17] ZHANG, Z., WANG, Q. Application status and prospects of 5G technology in distribution automation systems. *Wireless Communications and Mobile Computing* [online]. 2021, **2021**, 5553159. ISSN 1530-8669, eISSN 1530-8677. Available from: https://doi.org/10.1155/2021/5553159
[18] XIAO, Y., ZHANG, J., JI, Y. Resource-efficient slicing with topology-level protection in optical access/aggregation networks for 5G and beyond. In: 2021 Optical Fiber Communications Conference and Exhibition OFC: proceedings [online]. IEEE. 2021. ISBN 978-1-943580-86-6, p. 1-3. Available from: https://doi.org/10.1364/OFC.2021.W1F.4
[19] AMATO, E., TONINI, F., RAFFAELLI, C., MONTI, P. A resource sharing method for reliable slice as a service provisioning in 5G metro networks. In: 2021 International Conference on Optical Network Design and Modeling ONDM: proceedings. 2021. ISBN 978-3-9031-7633-1, p. 1-3.
[20] WANG, X., LU, X., FU, M., LIU, J., YANG, H. Optimization for survivable 5G network slice provisioning with augmented infrastructure. In: 2021 9th International Conference on Communications and Broadband Networking: proceedings [online]. 2021. ISBN 978-1-4503-8917-4, p. 192-196. Available from: https://doi.org/10.1145/3456415.3456446
[21] HOSSAIN, A., ANSARI, N. 5G multi-band numerology-based TDD RAN slicing for throughput and latency sensitive services. *IEEE Transactions on Mobile Computing* [online]. 2021, Early Access. ISSN 1536-1233, eISSN 1558-0660. Available from: https://doi.org/10.1109/TMC.2021.3106323
[22] ZHOU, H., ELSAYED, M., EROL-KANTARCI, M. RAN resource slicing in 5G using multi-agent correlated q-learning. In: 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC: proceedings [online]. IEEE. 2021. ISBN 978-1-7281-7587-4, eISBN 978-1-7281-7586-7, ISSN 2166-9570, eISSN 2166-9589, p. 1179-1184. Available from: https://doi.org/10.1109/PIMRC50174.2021.9569358
[23] KAYTAZ, U., SIVRIKAYA, F., ALBAYRAK, S. Hierarchical deep reinforcement learning based dynamic RAN slicing for 5G V2X. In: 2021 IEEE Global Communications Conference GLOBECOM: proceedings [online]. IEEE. 2021. ISBN 978-1-7281-8105-9, eISBN 978-1-7281-8104-2, p. 1-6. Available from: https://doi.org/10.1109/GLOBECOM46510.2021.9685588