SECURED VERTICAL HANDOFF USING MACHINE LEARNING TECHNIQUE IN 5G WIRELESS NETWORKS

Abstract

The fifth generation (5G) networks are a popular standard that carries effective skills to conquer the tests of next generation wireless networks. Also, the 5G systems can support high data traffic by rendering high throughput and low latency towards the massively connected nodes. Here, handover is highly significant for data processing, portability and real time data creation in mobile technologies. With the 5G entrance, the cellular network has become a completely heterogeneous network (HetNet). The Software Defined Network (SDN) concept is used in 5G HetNets for better mobility management. Most existing research works have concentrated on handover authentication, but those works are often prone to re-authentication issues and increased handover delay. Therefore, to overcome the re-authentication process and provide users with better services, a novel handover authentication mechanism using deep learning is proposed. Initially, the 5G data attack and normal data are collected, and the malicious and non-malicious users are classified using the Convolution Stacked long short term memory network model. To improve handover process and resist network attacks, only the non-malicious user data are authenticated through the key generation and the 5G Handover-Authentication and Key Agreement (5G_AKA) protocol. The process of encryption and decryption are performed using Extended Elliptic curve cryptography (Ex_ECC).

Authors

S. V. Saboji
Professor
Computer Science and Engineering
Basaveshwar Engineering College
Bagalkot, Karnataka, India.
sabojishivakumar@gmail.com

G. B. Chittapur
Assistant Professor
Computer Science and Engineering
Basaveshwar Engineering College
Bagalkot, Karnataka, India.
gbchittapur@gmail.com

Shivanand V. Manjaragi
Assistant Professor
Computer Science and Engineering
Hirasugar Institute of Technology
Belagavi, Karnataka, India.
shiva.vm@gmail.com

I. INTRODUCTION

The 5G networks possess increased capacities and data rates that recommend over applications including mobile banking and Internet of Things (IoT) [1]. The 5G cellular technology intends to realize the next generation network where the devices, machines and objects employ together [2-3]. The emergence of sensor devices, data exchange, sharing, sensing and analysis of gathered data to render enhanced facilities are gaining high priorities towards daily life activities. As highly sensitive data are exchanged in several applications, privacy and security schemes are necessary for deployments [4]. One of the major focus of 5G networks is huge accessibility of several users with enhanced communication rates [5]. The concurrent association of diverse cell types with differing software configurations generates heterogeneous networks (HetNets) in 5G. The immense participation of users involves numerous diversity in 5G HetNet because of lower coverage and processing ability.

In 5G-HetNet, the user devices cannot directly link over out dated cellular base stations accountable for geographical cells [6-7].The providence of security services and network administration inside heterogeneous cells are challenging since the user equipment (UE) may often leave one cell to another.5G requires taking into account the accept to suppress these consequences, 5G separates the standard cells over reduced geographical areas and possess diverse small cells including femtocell, picocell and microcell in 5G networks for network access support [8-9]. The issues of blind spot signal coverage, hotspot capacity improvement can be effectively solved through 5G HetNets and thereby the resource utilization and capacity enhancement of wireless mobile communication systems can be enhanced [10]. As intense of user devices are connected towards the network, the 5G HetNet density will be highly maximized.

The deployment density of diverse forms of less power nodes in case of different wireless transmission approaches will reach 10 times more than the coverage area [11].The huge small cell utilization and coexistence of numerous heterogeneous network nodes are subjected to adverse challenges in handover based security aspects and network administration [12-13]. In case of 5G HetNets, handover based security is very vital for generating real time data, processing of data in mobile technology and portability of data. The cellular network has turned as the whole HetNet because of integrated user networks with mobile devices with the entrance of 5G technology [14]. The recently advanced technologies like Software Defined Networks (SDN) has gained improved attention in the development of next generation wireless networks [15]. The control plane is detached from SDN data plane whereas it's controlling section meet the control requirements in 5G with better management of network flexibility and programmability.

The SDN controller is recommended for the whole cell control whereas the SDN switch deals with the behavior variations and data transfer in the network based on the controller commands [16-17]. The combination of SDN in 5G is highly beneficial because increased scalability is needed in the future mobile networks [18].The SDN flexibility can render greater benefits towards 5G applications with respect to machine to machine (M2M), human to human (H2H) and quality of service (QoS) communications [19]. The indulging of user devices with enormous diversity tends the handover security more complicated especially when the resource constrained 5G users possess less processing power. Hence to maintain the handover security, trust between the users are highly necessary to perform an

authentication process [20]. The rapid and secured connection is needed with the elimination of re- authentication process among handover operators between the heterogeneous cells possessing less delay.

1. Contributions of the Proposed Research Work are given as Follows

- To introduce an efficient Handover Authentication Mechanism Using Deep Learning (DHan_Auth) to enhance classification accuracy, handover process and security.
- To develop a novel deep learning approach called Convolution Stacked LSTM network model (Conv_SLSTM) for categorizing the malicious and non-malicious users effectively.
- To provide better handover authentication process for generating keys using 5G Handover-Authentication and Key Agreement (5G_AKA) protocol and data exchange using Extended Elliptic curve cryptography (Ex_ECC).
- To compare the performances of proposed work with the existing state-of-the-art methods in terms of different performance metrics to prove the performance superiority of the proposed method.

II. LITERATURE SURVEY

The incorporation of SDN in the 5G cellular network was performed by Monira et al. [21] in order to render better handover management and simplify the HetNets. To minimize the handover delay in the simplified form of HetNet, pre-authentication and idle time scanning were utilized. The network access was assured through permissible network components by the authentication policy. The device to device communication was considered during the handover process. During inter-domain reactive handover, 42% of the delay was optimized and 50% of lesser communication overhead was analysed. The latency can be greatly minimized in the mobility management approaches but effective handover solution cannot be attained.

Salim et al. [22] presented an effective, rapid handover authentication (HO-Auth) scheme for device authentication using deep learning (DL). The major objective of this approach was to ensure that the blockchain decentralized networks obtain data from legal devices and prevents the cloud applications from corrupted data. For immediate authorization, a user profile based system was generated. The model was trained through the channel state information (CSI) over the movement pattern of user and identifies the malicious users who are employing to be honest users. When the profile was retrained based on the user movement, the identification accuracy was maximized in to 95% but there exists high authentication delay.

An evolutionary approach that utilizes the fuzzy model was developed by Divakaran et al. [23] for handover regulation and key management to enhance the authentication performance. During the authentication of nanocore technology based 5G networks, the delays and complexities were minimized. When the model is trained with significant attack data, the attacks can be mitigated and validation was performed. The performances like communication overhead, space complexities and handover latencies were evaluated. Secured authentication of input messages and network users against diverse forms of attacks were promoted in mobile health programs. But the communication overhead was too high in

this research.

Yazdinejad et al. [24] proposed an effective authentication approach that adopted SDN and block chain based approaches to eradicate the re-authentication problems. The authentication process was employed in repeated handover among the heterogeneous cells. The presented approach was effectively designed to promote minimized delay and highly suitable for 5G network. The users can be switched with less delay across heterogeneous cells utilizing the private and public keys rendered by the block chain component with privacy protection. The main advantage of this research work was less authentication handover delay but the major issue was increased consumption of energy.

In Long Term Evolution network, an SDN based centralized solution was promoted by Emran et al. [25] for handover management. In this research work, the handovers are managed by SDN controller that holds the whole network management track. The flow entries were dictated to the open flow switches in the SDN network. The two UEs were associated over two evolved nodes whereas one UE undergone handover from one evolved node to another. The data rate of the running application can be widely enhanced with reduced delay. The accuracy of handover evaluations were influenced because of high handover probability and the handover facilities were not convincing.

Zhang et al. [26] proposed a Robust and Universal Seamless Handover (RUSH) authentication protocol for 5G HetNets for addressing universality and anonymity issues. The anonymous mutual authentication with key agreement were enabled for handovers through trapdoor collision property exploitation of chameleon hash functions and block chain tamper-resistance. In case of all different mobility conditions, the universal handover authentication can be attained through RUSH. The authentication can be exemplified through network handover and consistency. But the authentication cost and transmission overhead were found to be very high.

A 5G key management and handover protocol was proposed by Nyangaresi et al. [27] to conquer certain performance and security issues. The protocol presented in this paper acts as a multi criteria strategy that utilized power density, path loss, call blocking probability, traffic intensity and velocity as handover triggering parameters. The performances like communication overheads, handover latencies, space complexity and total number of executed handovers were analysed. But the protocols designed were not efficient in energy parameter and the mobility was not managed effectively.

Ozhelvaci et al. [28] focused on seamless and secure handover authentication mechanism for promoting rapid mutual authentication. A robust handover authentication protocol called Extensible Authentication Protocols- Transport Layer Security (EAP-TLS) was presented in this work. The protocol is dependent upon the public key infrastructure and it utilizes the user certificate whereas the communication takes place between the authentication server and user equipment. The major drawback found in this research was, the handover facilities were not convincing.

Yang et al. [29] introduced wireless link signatures decided through user location in the form of handover authentication data in 5G SDN based HetNets. As the secure context information (SCI), the wireless channel characteristics between the serving access point (AP)

and user were extracted. The authentication performance associated to various attributes were analysed to demonstrate the authentication strength. Through proper decision threshold settings and sub optimal performance derivation, optimal performance can be obtained. The latency and overhead were analysed and compared with existing handover authentication mechanisms. But the simulation time and latency were found to be very high.

Tong et al. [30] proposed a mobility-aware seamless handover process dependent upon multipath transmission control protocol (MPTCP) in SDN based 5G enabled nanocore technologies. This work comprises of three procedures including network selection, location prediction and handover execution. Initially, the user location was predicted using an echo state network. The target network was chosen using fuzzy analytic hierarchical process (FAHP) algorithm and the seamless handover was realized using MPTCP based handover process. The major drawback faced in this research was increased time delay and loss rates.

When there exists huge amount of data to be transferred, the evaluation of direct interactions consumes more time and computationally complex as there may involve huge operations to be done. Diverse networking attacks occur because of ineffective authentication in SDN based 5G HetNets. The signaling overhead becomes high with increased energy consumption during communication. For effective classification of malicious and non-malicious data, machine learning (ML) approaches are employed in most of the works. Compared to machine learning, DL possess greater significance in enhancing the classification accuracy because of high training ability. Hence, the mutual authentication between 5G users and gNBs is required to withstand attacks. To overcome the existing issues, an effective handover authentication mechanism using DL is proposed to obtain better QoS.

III. PROPOSED METHODOLOGY

As the core technology aspect of 5G networks, higher data rates can be provided through HetNet over real time applications. The densification of 5G network environment overcomes the signal strength coverage issues in blind spots and maximizes the data necessities in high density areas. But in most of the existing research works, security attacks are found to be the major concern because of improper authentication. The major issue developed in SDN based 5G HetNet is rapid authentication for linking devices between diverse gNBs. The maximized latency due to slower handover authentication permits an attacker to launch security attacks that influence the data security and QoS in heterogeneous cells.

Initially the 5G data are collected whereas the SDN based 5G HetNets is considered with the initialization of 5G users and gNB. To overcome the re-authentication process and to provide better services to the users, a novel DHan_Auth model is proposed. The initial step is to classify malicious and non-malicious data through DL model called Conv_SLSTM. To enhance handover process and security against network attacks, only the non-malicious user data are authenticated through key generation and 5G_AKA protocol. The data exchange process is carried through Ex_ECC whereas the process of encryption and decryption can be undertaken. After the successfulauthentication, the BS ensures related QoS to the users.The input data is initially fed into the convolutional layers of Conv_SLSTM whereas the significant deep features can be extracted. The extracted features are fed over the pooling layer whereas the unwanted features can be diminished. Then, the features are processed

using SLSTM model and finally the normal and attack are classified effective using the fully connected layer.

- **Convolutional Layer:** The conforming features of an input data is designated as the outline of convolutional layer. In this layer, the original data form is filtered and a convolution operation is carried. Through this layer, the deep data features can be extracted and fed over the pooling layer.

- **Pooling Layer:**The pooling layer progressively minimizes the feature size to decrease the number of parameters, computational complexity and to manage the over fitting problems. The pooling layer encapsulates the features from the convolution layer and also it controls the feature resolution to improve the steadiness.

- **SLSTM Layer:**The SLSTM layer is used to learn the long term dependencies of data to overcome the vanishing gradient issues and to enhance the training process.

- **Fully Connected Layer:** In case of classification problems, the fully connected layer integrates the features for data classification.

1. **System Model:** To mitigate the limitations in SDN based 5G HetNets, the proposed research work presents an Efficient Handover Authentication Mechanism Using DL model. Figure 1 demonstrates the system model of proposed methodology.

   SDN Controller

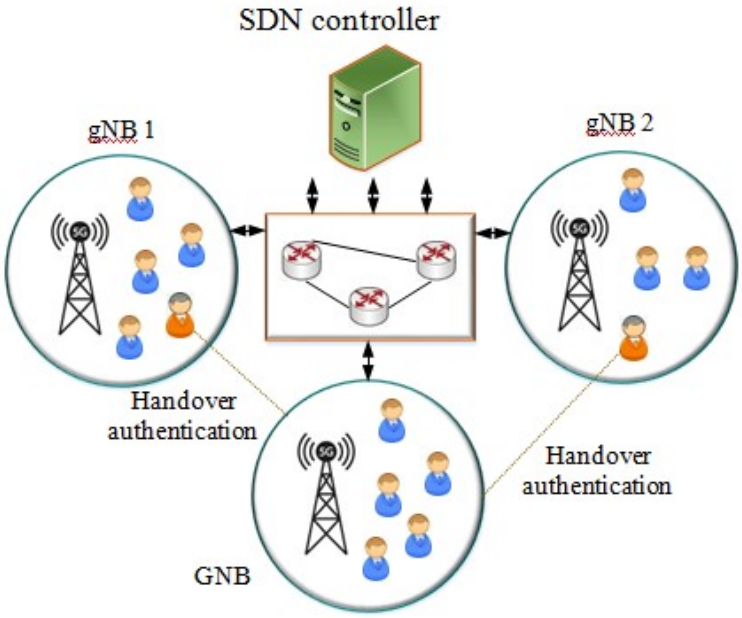

Figure 1: Schematic Workflow of Proposed Model

The number of users considered in the simulation of proposed experiment is 200 and 3 gNBs are deployed. An SDN controller is called as the domain controller that is responsible for process coordination of authoritative domain. It can trace any form of network equipment like end devices and switches within its domain. The open flow enabled SDN switch also called as cell switch is accountable for cell management. The switches manage the 5Ggeographical cell under the supervision of SDN controller. It links diverse end users within the geographical coverage area.

2. **Data Acquisition**: In the proposed DHan_Auth model, 5G attack detection dataset is employed as the input and it comprises of intercepted 5G network data. The dataset includes both normal and attack datathat are created in a simulated environment[31].The data are gathered through an internet associated linux machine running a 5G core network implemented with open source free 5G core software. To capture all network traffic on the 5G core machine interfaces, Wireshark application is used.

3. **Normal Data Model Description:** The normal data is categorized into data collection with one user equipment simulation and data collected using two user equipment simulations.

4. **Attack Data Model Description:** The malicious data includes ten forms of attacks that come under three major categories like denial of service (DOS), reconnaissance and network reconfiguration. The Access and Mobility Management Function Looking for Unified Data Management (ALU) attack, Get All Network Functions (GAF) attack, Get user data (GUD) attack, Automatic Redirect with Timer (ART) and random data dump (RD) attack comes under reconnaissance attack. The Fake access and mobility management function Insert (FAI) attack, Fake access and mobility management function Delete (FAD) attack, Random access and mobility management function Insert (RAI) attack, Random access and mobility management function delete (RD) attack comes under the network reconfiguration attacks. The Crash Network Repository Function Attack (CN) comes under the DOS attacks**.**

5. **Model Training and Data Classification:** Using the proposed classifier model, the malicious and non-malicious user data can be precisely classified. The framework of the proposed model has been provided clearly in the upcoming sub-section**.**

6. **Framework of the Proposed Model:** in DHan_Auth model, only the normal data needs to be encrypted and authenticated for better services. To eradicate the attack data, the normal and attack data are initially classified using Conv_SLSTM model. The input data are fed as the input towards convolution layers for extracting some of the relevant features whereas the obtained features are fed as the input to stacked LSTM structure. The computational complexity can be greatly minimized through high parameter range settings like input bias, output bias and learning rate. In LSTM cell, a memory cell is integrated that can obtain the information present in memory for longer duration. As an advanced version of RNN, vanishing gradient problem can be effectively minimized and long term dependencies can be acquired in LSTM [32]. There are three gates included in LSTM are input gate, output gate and forget gate. The neurons in LSTM include three gates and memory cell. The fundamental design of LSTM is portrayed in Figure 2.

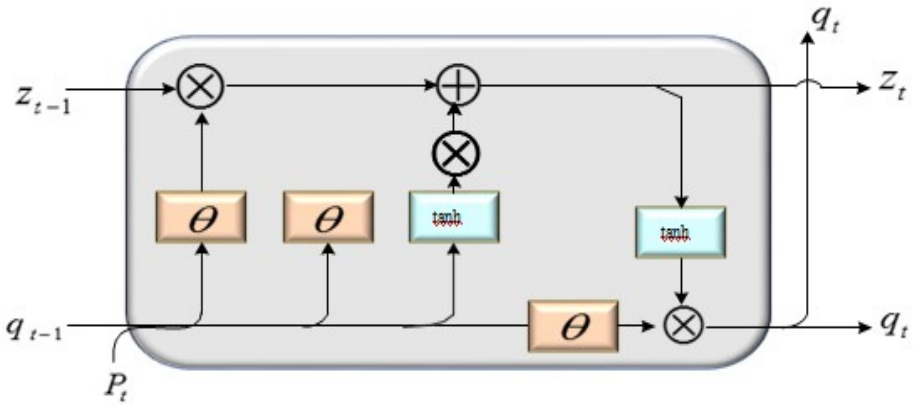

Figure 2: LSTM Architecture

To determine the information quantity from the previous layer $^{qt-1}$ which has to be forgotten dependent upon the current input, forget gate is utilized.

Even though, LSTM possess a robust approach but suitable information cannot be utilized from the future data. Hence, stacked LSTM network that includes two separate hidden LSTMs in opposite directions to the similar output has been utilized. The architecture of Conv_SLSTM model is illustrated in Figure 3.

7. Stacked LSTM Model

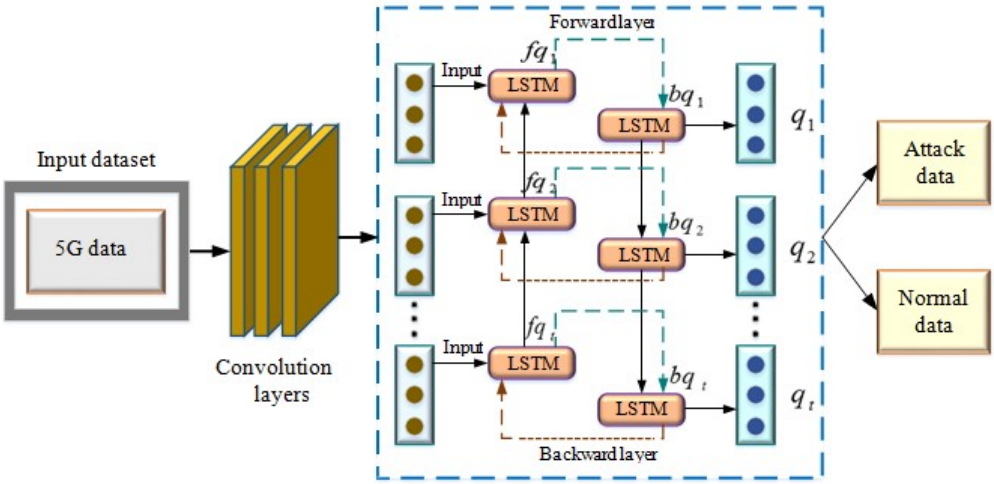

Figure 3: Conv_SLSTM model architecture

8. **Handover Authentication:** The public and private keys are initially generated using RSA [33] model and the non-malicious data are authenticated using 5G_AKA protocol. The data exchange process is carried through Ex_ECC whereas the process of encryption and decryption can be undertaken. To overcome the **re-authentication issues and** security vulnerabilities, 5G_AKA protocol is employed. The presented protocol

comprises of three phases that are given as follows.

- Preparation phase
- Handover Initialization phase
- Handover authentication phase

The definition of Ex_ECC and security assumptions are implied in the preparation phase. The user equipment is verified at Access and Mobility Management whereas the node N1transfers the handover message towards the user equipment for effective communication during the initial authentication phase. When the user equipment enters the coverage area of node N2 from node N1, the user equipment and the node N2 performs the handover authentication process.

9. **Preparation Phase:** The ECC [34] acts as a public key encryption approach that depends upon the elliptic curve theory. The Ex_ECC denotes a curve based approach that possesses appropriate base point evaluated from the functions of prime numbers. As the ECC approach is harder to implement, the chances of implementation errors are more and thereby, the algorithm security is reduced. To improvise the security of the algorithm, Ex_ECC is used in the proposed work to generate the secret keys. The generated secret is integrated with the encryption formula and is subtracted during decryption. The intricacy of the two phases are augmented in this way and if the encryption-decryption intricacy is elevated, original data detection tends to be complex. This process can automatically enhance the data security.

10. **Handover Initialization Phase:** During this phase, the user equipment is authenticated at AMF, AUSF and ARPF through the execution of proposed protocol. After the successful user equipment verification, the exchanges the secret session key towards N1 whereas it send the message to user for future handover process.

11. **Handover Authentication Phase:** When the user equipment enters into the coverage area of node N 2 , mutual authentication and key agreement procedure is commenced between N 2 and user equipment. The interaction diagram for handover authentication process is described in Figure 4.

The handover authentication delay can be reduced by overcoming the reauthentication issues using 5G_AKA protocol. When the user enters from one location to another location, the coverage area deviation can be overcome and the user can authenticate the data efficiently. Using the proposed DL model, only the non-malicious users are authenticated and so, the attack data cannot be intruded during communication. By restricting the malicious users into the network, several data attacks can be avoided and so the handover delay is also reduced.

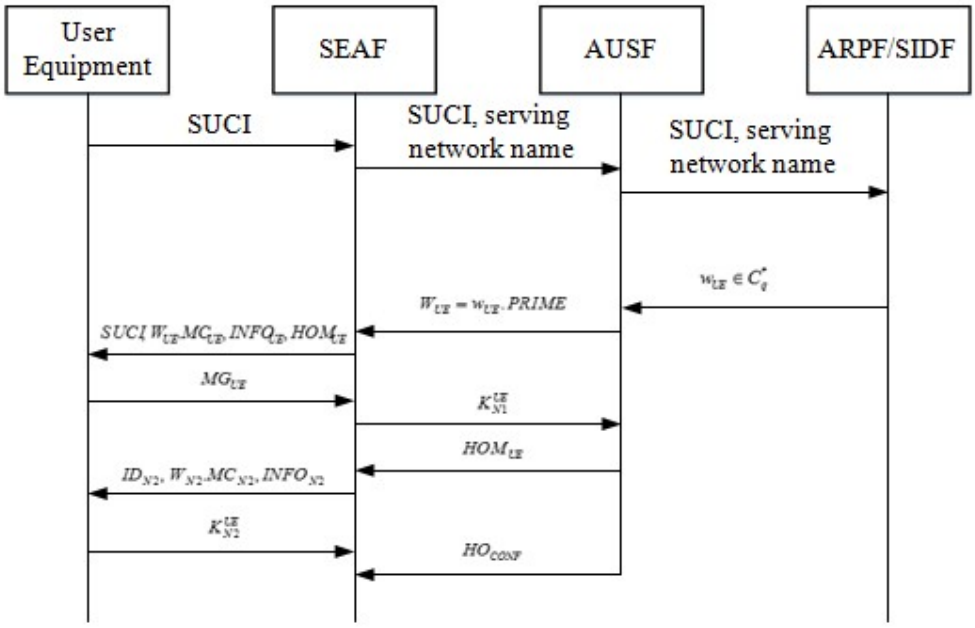

Figure 4: Handover Authentication Process

IV. CONCLUSION

In this work, the DHan_Auth approach is proposed for better handover management and key management in SDN based 5G HetNets. The issues of handover delay and re-authentication are highly concentrated to promote an effective handover authentication process. The 5G data were collected initially and to enhance the data security, the classification of attack data and normal data will be performed using DL based Conv_SLSTM model. On considering the network attack resistance and better handover process into an account, only the normal data are authenticated by key generation using 5G_AKA protocol. The data exchange process is carried out using Ex_ECC whereas the process of encryption and decryption are performed. The performances like handover latency, accuracy, precision, recall, RMSE and F1 score are analysed.

REFERENCES

[1] Yan, Xiaobei, and Maode Ma. "A lightweight and secure handover authentication scheme for 5G network using neighbour base stations." Journal of Network and Computer Applications 193 (2021): 103204.
[2] Chen, Zhonglin, Shanzhi Chen, Hui Xu, and Bo Hu. "A security authentication scheme of 5G ultra-dense network based on block chain." IEEE Access 6 (2018): 55372-55379.
[3] Yang, J., Ji, X., Huang, K., Chen, Y., Xu, X., and Yi, M. (2019). Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet. IET Communications, 13(2), 144-152.
[4] Ren, Z., Li, X., Jiang, Q., Cheng, Q., and Ma, J. (2021). Fast and Universal Inter-Slice Handover Authentication with Privacy Protection in 5G Network. Security and Communication Networks 2021.
[5] Sangeetha, D., Selvi, S., and Keerthana, A. (2022). A Trust-Based Handover Authentication in an SDN 5G Heterogeneous Network. In Computer Networks and Inventive Communication Technologies, Springer, Singapore, 841-852.
[6] Hojjati, M., Shafieinejad, A., and Yanikomeroglu, H. (2020). A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks. IEEE Access 8, 216461-216476.
[7] Yang, H., Liang, Y., Yuan, J., Yao, Q., Yu, A., and Zhang, J. (2020). Distributed blockchain-based trusted

multidomain collaboration for mobile edge computing in 5G and beyond. IEEE Transactions on Industrial Informatics 16(11), 7094-7104.

[8] Zhang, Y., Deng, R., Bertino, E., and Zheng, D. (2019). Robust and universal seamless handover authentication in 5G HetNets. IEEE Transactions on Dependable and Secure Computing.

[9] Kumar, A., and Om, H. (2018). Handover Authentication Scheme for Device-to-Device Outband Communication in 5G-WLAN Next Generation Heterogeneous Networks. Arabian Journal for Science & Engineering (Springer Science & Business Media BV) 43(12).

[10] Alezabi, K.A., Hashim, F., Hashim, S.J., Ali, B.M., and Jamalipour, A. (2020). Efficient authentication and re- authentication protocols for 4G/5G heterogeneous networks. EURASIP Journal on Wireless Communications and Networking 2020, 1-34.

[11] Cao, Jin, Maode Ma, Yulong Fu, Hui Li, and Yinghui Zhang. "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets." IEEE transactions on dependable and secure computing 18, no. 3 (2019): 1182-1195.

[12] Yang, Jing, Xinsheng Ji, Kaizhi Huang, Yajun Chen, Xiaoming Xu, and Ming Yi. "Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet." IET Communications 13, no. 2 (2019): 144- 152.

[13] Duan, Xiaoyu. "Software-defined Networking Enabled Resource Management and Security Provisioning in 5G Heterogeneous Networks." PhD diss., The University of Western Ontario (Canada), 2017.

[14] Ozhelvaci, Alican, and Maode Ma. "Secure and efficient vertical handover authentication for 5G HetNets." In 2018 IEEE international conference on information communication and signal processing (ICICSP), pp. 27-

[15] 32. IEEE, 2018.

[16] Lone, Tufail A., Aabid Rashid, Sumeet Gupta, Sachin Kumar Gupta, DuggiralaSrinivasa Rao, MohdNajim, Ashutosh Srivastava, Abhishek Kumar, Lokendra Singh Umrao, and AchintyaSinghal. "Securing communication by attribute-based authentication in HetNet used for medical applications." EURASIP Journal on Wireless Communications and Networking 2020 (2020): 1-21.

[17] Ozhelvaci, Alican, and Maode Ma. "A Robust Vertical Handover Authentication for SDN based 5G HetNets."

[18] Abdelhady, M. Said, W. Anis, A. Abd-Elhafez, H. Eldemerdash, and AmrAbdelaziz. "Novel Framework for Secure Handover Authentication Protocol for 5G Mobile Network."

[19] Lai, Chengzhe, Yixiao Ma, Rongxing Lu, Yinghui Zhang, and Dong Zheng. "A novel authentication scheme supporting multiple user access for 5G and beyond." IEEE Transactions on Dependable and Secure Computing (2022).

[20] Nyangaresi, Vincent Omollo, Anthony Joachim Rodrigues, and SilvanceOnyangoAbeka. "Machine learning protocol for secure 5G handovers." International Journal of Wireless Information Networks 29, no. 1 (2022): 14-35.

[21] Zhang, Yinghui, Robert H. Deng, Elisa Bertino, and Dong Zheng. "Robust and universal seamless handover authentication in 5G HetNets." IEEE Transactions on Dependable and Secure Computing 18, no. 2 (2019): 858-874.

[22] Monira, Shaikhum, UpamaKabir, MosarratJahan, and Uchswas Paul. "An Efficient Handover Mechanism for SDN-Based 5G HetNets." Dhaka University Journal of Applied Science and Engineering 6, no. 2 (2021): 49- 58.

[23] Salim, Mikail Mohammed, VimalShanmuganathan, Vincenzo Loia, and Jong Hyuk Park. "Deep learning enabled secure IoT handover authentication for blockchain networks." Hum. Cent. Comput. Inf. Sci 11 (2021): 21.

[24] Divakaran, J. S. K. P. G. B. M. D. S. N. M. S., S. K. Prashanth, GouseBaig Mohammad, Dr Shitharth, Sachi NandanMohanty, C. Arvind, K. Srihari, Yasir Abdullah R, and VenkatesaPrabhuSundramurthy. "Improved handover authentication in fifth-generation communication networks using fuzzy evolutionary optimisation with nanocore elements in mobile healthcare applications." Journal of Healthcare Engineering 2022 (2022).

[25] Yazdinejad, Abbas, Reza M. Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks." IEEE Transactions on Network Science and Engineering 8, no. 2 (2019): 1120-1132.

[26] Emran, Muhammad, VijeyThayananthan, Muhammad Umair, Ivan Kotuliak, Muhammad Shuaib Qureshi, and Muhammad Bilal Qureshi. "The Handover and Performance Analysis of LTE Network with Traditional and SDN Approaches." Wireless Communications and Mobile Computing 2022 (2022).

[27] Zhang, Yinghui, Robert H. Deng, Elisa Bertino, and Dong Zheng. "Robust and universal seamless

handover authentication in 5G HetNets." IEEE Transactions on Dependable and Secure Computing 18, no. 2 (2019): 858-874.

[28] Nyangaresi, Vincent Omollo, Anthony Joachim Rodrigues, and SilvanceOnyangoAbeka. "Neuro-fuzzy based handover authentication protocol for ultra-dense 5G networks." In 2020 2nd Global Power, Energy and Communication Conference (GPECOM), pp. 339-344. IEEE, 2020.

[29] Ozhelvaci, Alican, and Maode Ma. "Secure and efficient vertical handover authentication for 5G HetNets." In 2018 IEEE international conference on information communication and signal processing (ICICSP), pp. 27-

[30] 32. IEEE, 2018.

[31] Yang, Jing, Xinsheng Ji, Kaizhi Huang, Yajun Chen, Xiaoming Xu, and Ming Yi. "Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet." IET Communications 13, no. 2 (2019): 144- 152.

[32] Tong, Haonan, Tao Wang, Yujiao Zhu, Xuanlin Liu, Sihua Wang, and Changchuan Yin. "Mobility-aware seamless handover with MPTCP in software-defined HetNets." IEEE Transactions on Network and Service Management 18, no. 1 (2021): 498-510.

[33] Coldwell, Cooper, Denver Conger, Edward Goodell, Brendan Jacobson, Bryton Petersen, Damon Spencer, Matthew Anderson, and Matthew Sgambati. "Machine Learning 5G Attack Detection in Programmable Logic." In 2022 IEEE Globecom Workshops (GC Wkshps), pp. 1365-1370. IEEE, 2022.

[34] Drumond, Rafael Rego, Bruno A. Dorta Marques, Cristina Nader Vasconcelos, and Esteban Clua. "An LSTM recurrent network for motion classification from sparse data." In Proceedings of the 13th international joint conference on computer vision, imaging and computer graphics theory and applications, vol. 1, pp. 215-22. 2018.

[35] Minni, Rohit, Kaushal Sultania, Saurabh Mishra, and Durai Raj Vincent. "An algorithm to enhance security in RSA." In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1-4. IEEE, 2013.

[36] Liang, Haotian, Guidong Zhang, WenjinHou, Pinyi Huang, Bo Liu, and Shouliang Li. "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography." Applied Sciences 11, no. 12 (2021): 5691

