Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 3192 - 3198

Received 15 December 2020; Accepted 05 January 2021.

Slice-Based Integrity Authentication Scheme for Secure 5G User Equipment Communication

Sakthibalan Pandiyan*, Dr. Devarajan Krishnamoorthy

Department of Electronics and Communication, Annamalai University, Tamil Nadu, India

Abstract

The Fifth Generation (5G) communication networks offer reliable communication and information exchange through terahertz bandwidth and Machine Type Communications (MTCs). It integrates User Equipment (UE), infrastructure devices, cloud, software paradigms, etc., for providing uninterrupted services in heterogeneous environments. The user services are interrupted by bidding adversaries through infrastructure impersonations. In this article, a Slice-based Integrity Authentication Scheme (SIAS) is introduced for combating such attacks. The proposed scheme defines communication slices for each session for providing linear authentication. The interruption in communication is confronted by altering the authentication sequence for aiding concurrent slice-authenticated transmissions. This process relies on linear decision-making for reducing the adversary impact, communication overhead, and session delay for different UEs and slices.

Keywords—5G Communication, Authentication, Bidding Attacks, Decision-Making,Transmission Integrity

1. Introduction

Internet of Things makes a revolution worldwide by connecting physical objects. IoT Internet of Things (IoT) promising technology that attracts the research community's attention to ensure sensors, washing machines, smart phones etc., are all together connected to a common interface and the ability to communicate with each other [1]. Fifth Generation (5G) networks ensure the devices and services like enhanced Mobile Broadband (eMBB), Critical Communications, massive Machine Type Communication (mMTC), and network operation [2]. Authentication issues, authorization, and accounting issues (AAA) are ensured by the 5G cellular system's security mechanism for heterogeneously interconnected IoT devices. For efficient resource utilization, lightweight CoAP/UDP based IoT networks are designed with a contextual aware congestion control mechanism to enable the requirement of 5G new series [3].

To protect users from various attacks and to mitigate malware, smartphone operating system (OS) vendors like Microsoft, Apple, etc. Denial of service attacks based on signaling traffic is mitigated by protecting systems build within the devices [4]. Possible spoofing attack detection takes more effort in the existing literature, and it will not resume GPS receiver's normal operation, particularly in network's normal operation of PMU applications is not interrupted [5]. Spoofing countermeasures are used to detect attacks and mitigate their effect on resuming the conventional network operations. The clock bias and drift are estimated by Time Synchronization attack rejection and mitigation and network attacks. The effect of reported attacks is detected and mitigated in the receiver's position is not altered by the real-time rejection and mitigation of time synchronization attacks [6, 7].

2. Related Work

Kim et al. [8] proposed a 5G wireless P2MO backhaul security protocol: an adaptive approach. The proposed protocol provides integrity, confidentiality, security, mutual authentication, perfect forward secrecy, secure exchange of keys, etc., and prevents exhaustion attacks on resources effectively and securely. BAN logic and Scyther tool are used for analysis purposes. The proposed protocol is compared with other protocols to prove its better performance.

An efficient authentication and re-authentication protocol for 4G/5G heterogeneous networks is suggested by Alezabi et al. [9]. User identities are protected, and the proposed work reduces the AS (authentication server) burden. The analytical model is used to achieve better performance. The

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 3192 - 3198

Received 15 December 2020; Accepted 05 January 2021.

handover cost and delay, energy consumption is also reduced. Various types of secrecy attacks and authentication are prevented, secured by the verification tools.

Fu et al. [10] recommended a secure SDN-based multi-RANs architecture for future 5G networks. The bandwidth detection and forward packets are managed efficiently by the proposed approach. The mobile device improves the data transmission rate RAN capabilities. The proposed framework developsseveral security models to list the security threats for protecting the proposed network. Ban logic is used to verify the security of the key exchange.

Braeken [11] considered symmetric key-based 5G AKA authentication protocol satisfying anonymity and unlinkability.The proposed algorithm is implemented based on symmetric key and cryptographic primitives in the USIM (universal subscriber identity module). The public key encryption is not required for hiding the identity in the proposed protocol. RUBIN logic is used to provide security.

A self-adaptive deep learning-based system for anomaly detection in 5G networks is used in [12]. The configuration of the cyber defense architecture is adapted to manage the traffic. The analysis and detection are done to optimize the computing resources. The diverse deep learning solutions determine the stability and performance of the proposed work. The result obtained shows that the proposed architecture adapts the automatic detection by gathering the network flow in UE (5G user equipment).

Efficient quantum-based security protocols are designed in [13] for information sharing and data protection in 5G networks. Two efficiently secure protocols are used to secure the data in the 5G network. The proposed architecture provides robustness, efficiency and security for various attacks through performance and simulation analysis. The proposed work is best in securing the applications in 5G networks.

Cao et al. [14] suggested anti-quantum fast authentication and data transmission scheme in 5G NB-IoT systems for massive devices.Authentication and data transmission is achieved by the proposed scheme using lattice-based homomorphic encryption. The proposed work obtains efficient performance.

Zhang et al. [15] modeled less multi-party authentication encryption for the NB-IoT terminal in 5G networks.The proposed work provides identity anonymity and non-repudiation along with achieving multi-party authentication. Data transmission and access authentication are combined in the proposed scheme. Access and mobility management validate and secure the data by proposed authenticated ciphertexts. Security analysis is used to analyze the proposed method for its efficiency and security.

3. Slice-based Integrity Authentication Scheme (SIAS)

The 5G communications rely on baseband signals for end-to-end data transfer. The integrity of the shared data is questionable due to bidding down attacks. These attacks degrade the quality and rate of the data exchange between the user equipment (UE). The resulting communication takes place in a low-level network with confined features. For addressing this attack, SIAS is proposed; the sharing intervals resliced with the independent authentication sessions. The session's length requires fixed keys for authentication, increasing the security by preventing communication complexity and adversary impact. The keys are generated using the UE supported public key cryptography functions. Let N denote the slices of the communication bestowed baseband B. The possibility of the transmitting UE to establish a link with the requesting UE is defined by equation (1)

$$\rho_T = \log_2\left[1 + \left(\frac{r-s}{r}\right) - (1-\rho_c)\right]$$

$$where\ \rho_c = \begin{cases} 1, if\ UE's\ communicate \\ 0, if\ UE halt \end{cases} \quad (1)$$

In equation (1), the variables r and s represent the communication request and its response between the UE. The variable ρ_c represents the communication probability for establishing the wireless links. The communication session (τ) is segmented into $\left(\frac{\tau}{N}\right)$ slices for each augmentation of a new service provider. This helps to retain concurrency and high-speed data transfer between the UE's. For each slice, the authentication follows linear decision-making to employ/ revoke the current

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 3192 - 3198

Received 15 December 2020; Accepted 05 January 2021.

sessions. This authentication makes use of baseband identification and capacity (ψ) of the $UE's$ for sharing information. If a change in capacity is reported, then the linear authentication is revoked, and concurrency is administered. The session is authenticated using a session ID; this ID is confined to the slice time.

$$\left.\begin{array}{c} S\_ID = H(\mathbb{R}) \\ N[S\_ID] = H[(S_k \oplus \mathbb{R}) \| \rho_T \| \rho_c] \\ and \\ Q_k = a \otimes H[S_{ID} || S\_ID] \end{array}\right\} \quad (2)$$

In equation (2), $H(.)$ is the public hash function, S_ID is the session identification, $\mathbb{R}$ is a random prime number.S_k is the session key, $a \in \mathbb{R}$ and Q_k is the private key. The validity of the key is retained until a new N is identified. The linear decision-making process generates N sequence for the identified slices. In all the slices, the authentication is performed as follows

$$\left.\begin{array}{c} \delta_{S\_ID} = \mathbb{R} * S_k * p \\ \delta(S\_ID, Trans) = Q_k \oplus S_k [S_s(S\_ID\ , D) || \delta_{S\_ID}] \end{array}\right\} \quad (3)$$

In equation (3), the variable p denotes communication data(D), session signature(S_S) is generated asQ_k. $N[S\_ID]$. In this case,$\rho_c = 0$ achieves two possibilities, namely$\rho_T = 1$ and 0. If $\rho_c = 1$ and $\rho_T = 1$ and $\rho_c = \rho_T = 0$ is experienced, then a formal transmission takes place. The case of$\rho_c = 1$ and $\rho_T = 0$ is also feasible due to the unavailability of the UE. Contrarily, the existence of$\rho_c = 0$ and $\rho_T = 1$ results in bidding wherein the baseband is exploited by an external UE. Therefore, the linear decision-making halts the current transmission and thereby performs Concurrent and non-linear authentication. The integrity verification for both the sequence of data communication between UE's varies for ensuring the base band's secure exploitation.

The secure transmission process is represented in Fig.1 for interrupting and non-interrupting N. In the secure non-interrupting transmission, the verification process is dependent on N such that every sequence is verified cumulatively. Contrarily, the initial acknowledgment is verified for the available interrupting sequence concurrently. The condition of$\rho_c = 1$ is verified for ensuring$\rho_T = 1$ such that available sessions (in a single slice) are verified. This verification requires high communication overhead, letting adversary impact influence the transmission. In this process of confining the adversary impact and communication overhead, concurrency and decision making play a vital role.

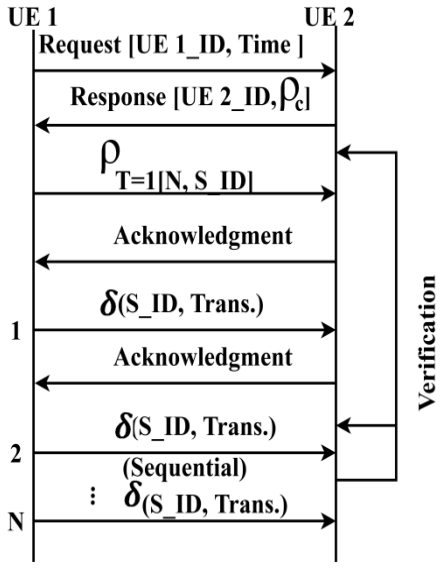

Fig 1(a) Non-Interrupting *N*

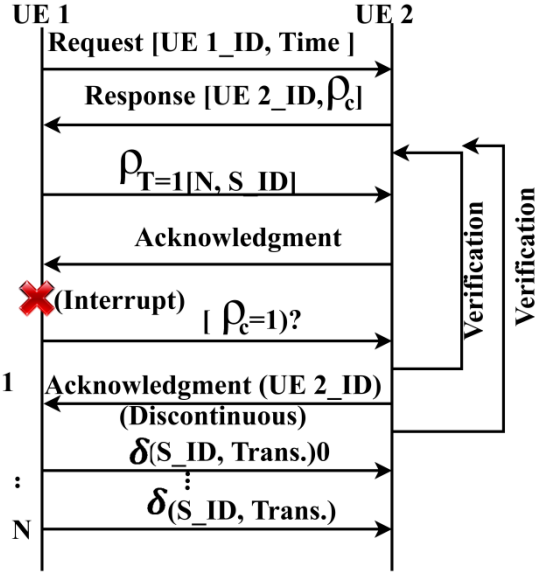

Fig. 1(b) Interrupting *N*

In the linear sequential process, the integrity is estimated as a utility value $(\mathcal{V})$ that is estimated using equation (4)

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 3192 - 3198

Received 15 December 2020; Accepted 05 January 2021.

$$\mathcal{V} = \begin{cases} \sum_{i=1}^{N} \rho_{c_i} W_i \times \left(\frac{s}{r}\right)_i \ \forall\ sequenctial\ N \\ \sum_{i=1}^{(N-T)} \rho_{T_i} (1-W)_i \left(\frac{r-s}{r}\right)_i + \sum_{(N-T)}^{N} (\rho_{c_i}) \left(\frac{s}{r}\right)_i, \forall\ interrupting\ N \end{cases} \quad (4)$$

For the authenticated sequence in equation (3), the utility value is estimated for all the transmission. The above utility of the transmitted sequence is verified for its integrity independent transmission. The above utility of the transmission sequence is verified for its integrity independently for the allocated weight (w). The weight relies on the ratio of $\left(\frac{s}{r}\right)$; If it is high, then W is high/ vice versa. This integrity verification requires both authentication and $\mathcal{V}$ features to ensure bidding-free data sharing. The process of sequential and interrupting integrity verification is expressed as in equation (5)

$$\left.\begin{array}{l} \delta(1,Trans).W_1 = Q_k.U_1 - H(\mathbb{R}) \\ \delta(2,Trans).W_2 = Q_k.U_2 - H(\mathbb{R}) \\ \vdots \\ \underbrace{\delta(N,Trans).W_N = Q_k.U_N - H(\mathbb{R})}_{Sequential\ N} \end{array}\right| \left.\begin{array}{l} \delta(1,Trans).\ (1-W)_{N-1} = Q_{k_{N-1}}.U_{N-1} - H(\mathbb{R})_{N-1} + (S_k \oplus \mathbb{R})_{N-1} \\ \delta(2,Trans).\ (1-W)_{N-2} = Q_{k_{N-2}}.U_{N-2} - H(\mathbb{R})_{N-2} + (S_k \oplus \mathbb{R})_{N-2} \\ \vdots \\ \underbrace{\delta(N,Trans).\ (1-W)_o = Q_{k_0}.U_0 - H(\mathbb{R})_0 + (S_k \oplus \mathbb{R})_0}_{Interrupting\ N} \end{array}\right\} \quad (5)$$

In the interrupting N verification $(1-W)_0$ indicates a final sequence of transmission. In this final and previous transmission,a sequence must be terminated such that no further integrity check is necessary. The first case of sequential N follows direct linearity, whereas the interrupting N pursues concurrent verification of the transmission. This can be represented as $[W_1|(1-W)_{N-1}]\|[W_2|(1-W)_{N-2}]\|\ldots\|[W_N|(1-W)_0]$ for verifying the integrity. This integrity verification process reduces communication (transmission) overhead and adversary impact by differentiating the sequential and interrupting N (concurrency).

4. Results and Discussion

The Performance of the proposed SIAS is verified using experimental analysis by deploying 50 UE's. The UE's are randomly dispersed in a $100m \times 100m$ network area operating at 2 Mbps bandwidth. In this experiment, $8-12$ UE's are initialized as bidding attackers and the maximum time for terminating a session is $2-4s$. For performance assessment, the metrics communication overhead, adversary impact, and session delay are considered. In the comparative study, the proposals of Cao. et al. [14] and Alezabai [9] are accounted.

4.1 Communication Overhead

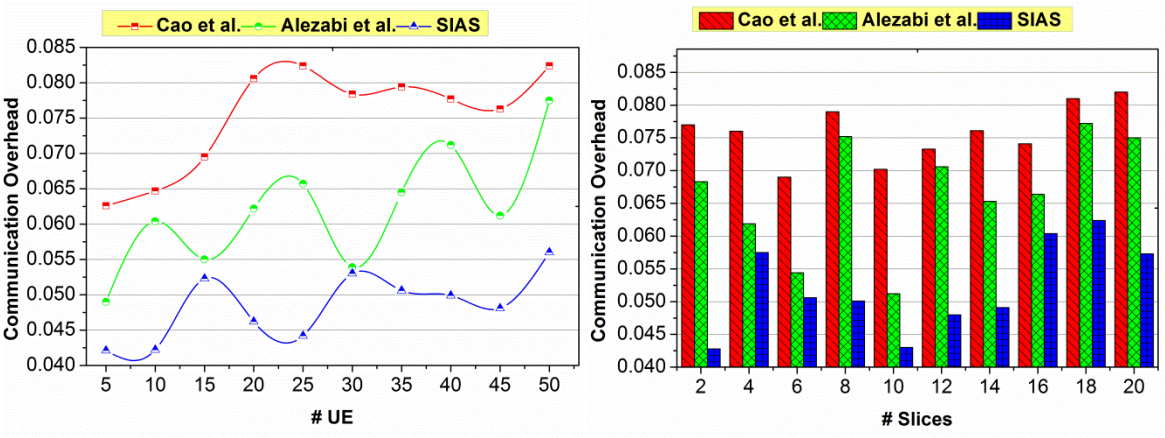

Fig. 2 Communication Overhead for (a) # UE and (b) # Slices

The proposed SIAS achieves less communication overhead for UE's and slices [Fig. 2(a) and 2 (b)]. This is because of the verification process using linear decision-making. In this decision-making process, the need for concurrency for mitigating bidding attacks is determined by verifying the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 3192 - 3198

Received 15 December 2020; Accepted 05 January 2021.

combinations of ρ_c and ρ_T.The authentication process relies on either of the dependencies (S_k orδ_{S_ID}) in both the sequential and interrupting N. Therefore, the need for reallocation of sessions is not required, reducing the communication overhead. Besides, the independent integrity verification for$[W_N|(1-W)_o]$ sequence reduces the grouped and complex transmission, controlling the overhead.

4.2 Adversary Impact

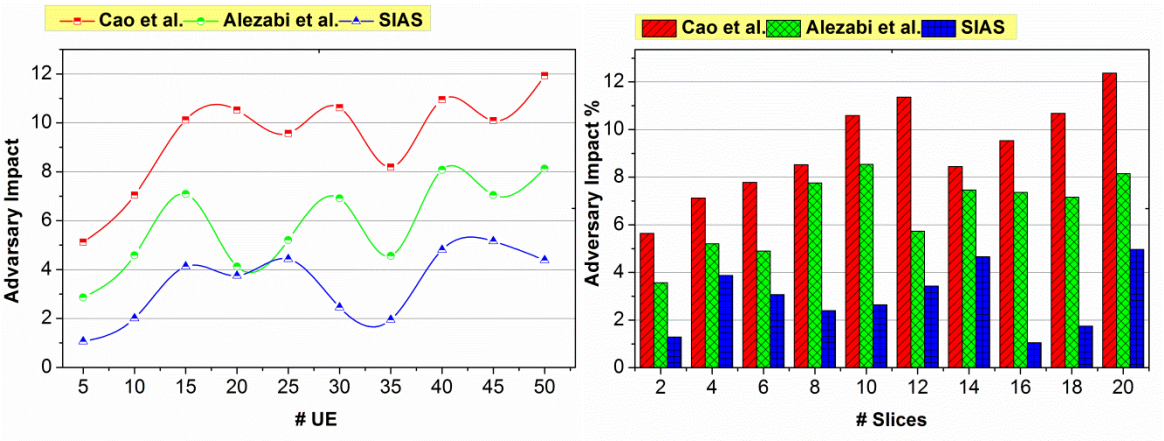

Fig. 3 Adversary Impact for (a) # UE and (b) # Slices

In Figs. 3(a) and 3(b), UE's and slices' adversary impact is compared. The proposed SIAS shows up less adversary impact by identifying the changes in the linear authentication sequence. The identified changes help to reinitiate the authentication process using$Q_k U_N$ (or)$Q_{K_o} U_o$ depending on the available sequence. Besides, the end-to-end security is verified using U in all the sequential and concurrent processes. From this point, either $N[S\_ID]$ (independent and sequential) (or)δ_{S_ID}(for concurrent) is used for providing better authentication. As the adversary's impact is detected at an early stage without change in transmission (further and preceding), the impact is controlled in both the slices and different UE's.

4.3 Session Delay

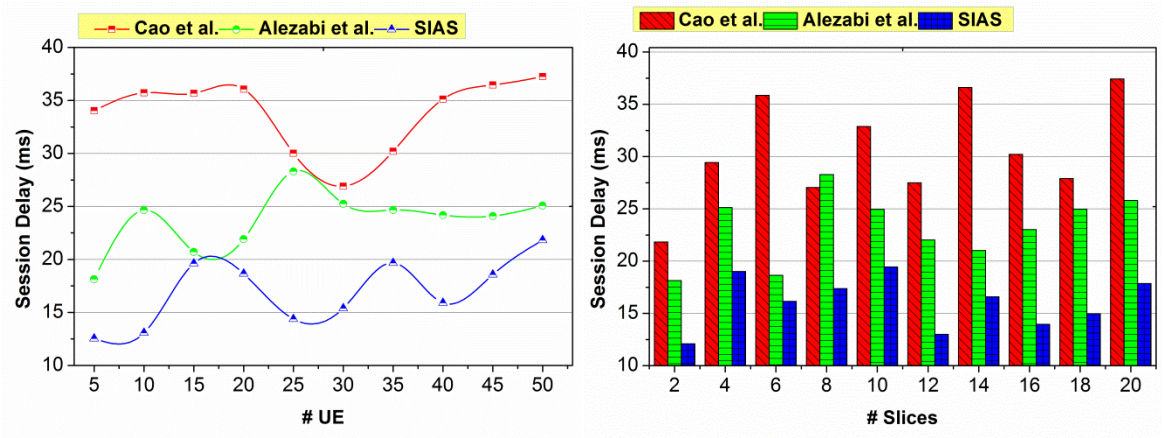

Fig. 4 Session Delay for (a) # UE and (b) # Slices

The count of reinitiated/ replaced sessions is less in the proposed SIAS method. In this method, additional sessions are not required due to bidding attacks. If an attack is detected, then concurrent authentication and integrity verification are performed. The concurrency requires non-sequential

authentication, reducing the transmission time. In this proposed authentication method, the need for overloaded sessions and failure is less, reducing the session delay. This process is unanimous for any UE and slices, as in Fig 4(a) and 4(b). The utility-based verification reduces the delay in the fore coming transmissions for all the UE.

5. Conclusion

This article introduced a slice-based integrity authentication scheme for improving the reliability of 5G UE communication sessions. The proposed scheme is designed to reduce bidding attacks over the UE transmissions in different sessions. For this purpose, it makes use of linear decision-making and utility-based authentication. In the authentication process, the integrity of the transmission is verified in independent and concurrent sessions. The session is differentiated into slices for providing reliable authentication irrespective of the user equipment. The decision-making process determines the modifications in the authentication for ensuring integrity for all the transmissions. The experimental analysis shows that the proposed scheme reduces communication complexity, adversary impact, and session delay for different UE and session slices.

References

[1] M.Anuradha, T.Jayasankar, PrakashN.B, Mohamed Yacin Sikkandar, G.R.Hemalakshmi, C.Bharatiraja,A. Sagai Francis Britto, "IoT enabled Cancer Prediction System to Enhance the Authentication and Security using Cloud Computing," *Microprocessor and Microsystems* (Elsevier 2021), vol 80, February, (2021) https://doi.org/10.1016/j.micpro.2020.103301

[2]A.Alnoman, A. Anpalagan, Towards the fulfillment of 5G network requirements: technologies and challenges,*Telecommunication Systems*, 2017,*65*(1), 101-116.

[3] X.Ji, K.Huang, L.Jin, H. Tang, C.Liu, Z.Zhong, M.Yi,Overview of 5G security technology,*Science China Information Sciences*,2017, *61*(8), 1-25.

[4] J.Xu, F. Li, K.Chen, F. Zhou, J.Choi, J. Shin, Dynamic chameleon authentication tree for verifiable data streaming in 5G networks. *IEEE Access*, (2017),*5*, 26448-26459.

[5]S.Zhang, Y.Wang, W. Zhou, Towards secure 5G networks: A Survey, *Computer Networks*,2019,*162*, 106871.

[6] S.Sicari, A.Rizzardi, A. Coen-Porisini, 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks*, 2020, *179*, 107345.

[7] Q.Wang, D.Chen, N. Zhang, Z. Qin, Z. Qin, LACS: A lightweight label-based access control scheme in IoT-based 5G caching context,*IEEE Access*,2017,*5*, 4018-4027.

[8]J.Kim, G.Choudhary, J.Heo, D. G.Duguma, I.You, 5G wireless P2MP backhaul security protocol: an adaptive approach, *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), 265.

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

[10] Y.Fu, Z. Yan, H. Li, X. L. Xin, J. Cao, A secure SDN based multi-RANs architecture for future 5G networks, *Computers & Security*,2017,*70*, 648-662.

[11] A. Braeken, Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability,*Computer Networks*, 2020,*181*, 107424.

[12] L. F.Maimó, Á. L. P. Gómez, . J. G. Clemente, F, Pérez, G. M.Pérez, A self-adaptive deep learning-based system for anomaly detection in 5G networks, *IEEE Access*, 2018, *6*, 7700-7712.

[13] A. A.Abd EL-Latif, B. Abd-El-Atty, S. E.Venegas-Andraca, W. Mazurczyk, Efficient quantum-based security protocols for information sharing and data protection in 5G networks,*Future Generation Computer Systems*, 2019, *100*, 893-906.

[14] J.Cao, P.Yu, X.Xiang, M. Ma, , &H.Li, (2019). Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system,*IEEE Internet of Things Journal*, *6*(6), 9794-9805.

[15] Y.Zhang, F. Ren, A. Wu, T. Zhang, J.Cao,D. Zheng, Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks, *IEEE Access*, 2019, *7*, 114721-114730.