Enhancing Secrecy Rate of UE with Dynamic Authentication and Access Control in 5G Communication Networks

Sakthibalan P. and Devarajan K.
Annamalai University, Annamalai Nagar -608002, Tamil Nadu
Email: balan1109@gmail.com; devarajan_lecturer@yahoo.com

***Abstract*—**In this paper, a dynamic access control and authentication framework for administering secrecy in 5G communication networks is presented. The framework is modeled to support both integrated and independent communication modes of user equipment with the heterogeneous access platform. Authentication framework is extended for normalized and time stamp based communication to mitigate the outage and delay constraints caused due to adversaries. The mode of communication authentication is secured on the basis of slot allocation and attribute based feature analysis. The authentication parameters are updated for both anomalies and legitimate user for ease of classification. The proposed method is found to achieve better secrecy through session key and attribute based authentication that is flexible for extended communications as well. The performance of the proposed framework is analyzed using the metrics: security and secrecy rate, outage probability and connection latency.

***Index Terms*—**5G communication networks, attribute based security, session key, slot allocation, user authentication

I. Introduction

The future advancement of telecommunication visualizes fifth generation or 5G wireless technology as an international communication standard. 5G is considered as the inheritance of present 4G networks providing improved radio resource and user adaption capacity. It supports interoperating features among device-to-device (D2D), human machine interaction, mobile communication users, etc. The reliability of the network is designed on the basis of low latency and efficient power expenses with better broadband and optical resource utilization [1]. Existing communication technologies such as massive multi-input multi-output (MIMO) systems, heterogeneous networks, D2D, software defined network (SDN), millimeter wave, etc. are finely packed into the 5G platform for providing seamless communication support and flexibility [2]. Radio and legacy equipment are correlated for 5G deployment and architecture design for improving the efficiency of communication. Multiple use case support design factors are modeled for 5G communications other than voice and data such as vehicular communications industrial communications, healthcare, defense, smart city projects, residential applications and etc. [2], [3].

With the deployment and applications of 5G communication networks, the challenges and issues related to security are prominent due to the heterogeneous characteristics of the environment. Administering security features is restricted to the resource constraint nature of the network and communication attributes of the user equipment (UE) [4]. On the basis of privacy policies, access control and vulnerabilities, the security issues in 5G networks is high. Authentication, secrecy, privacy, data freshness and integrity are some of the vulnerabilities that are to be mitigated from the communication environment. Next generation mobile networks (NGMN) require authentication and encryption kind of security measures for administering communication alliance with interoperable technologies and core networks [5]. Traffic management, user access control, network management, handoff procedures are the major security concentrated features in 5G. In this article we consider the importance of secrecy in 5G communications caused due to weak key procedures and dependent key distributions [6].

II. Related Works

Tian *et al*. [7] proposed a combination of two methods to improve the spectrum ability and security for the wireless communication networks. By integrating physical layer and full-duplex communication techniques, the authors have exploited wireless security. In the full-duplex techniques during synchronized transmission and response the spectrum ability can be improved. The problem of spectrum exploitation is addressed as mixed integer linear programming model. The introduced methods help to improve the security rate of the network.

Xiao *et al*. [8] introduced a two dimension negative jamming mobile communication method for detecting jamming attacks in mobile communications. Learning based security provisioning methods is implemented in the mobile tool to accomplish an ideal communication. This helps to classify legitimate user's radio frequency and jamming attacks in a precise manner. Using a Q-learning algorithm, the authors reduce the detection latency. Irrespective of the channels, this method helps to

Manuscript received August 25, 2019; revised January 3, 2020.
doi:10.12720/jcm.15.2.178-184

detect precise jammers to improve the radio resource utilization of the network.

To identify the network aberration in the real time is Maimó *et al*. [9] proposed a security solution by the coordinating the mobile edge computing (MEC) in the 5G networks. For the operator centric security results,security for information gathering and communication is inherited from the function of MEC. Network traffic and operation management are dynamically adapted as per the functions of MEC. The management of the current system operates on resources and it used by the proposed method of identification to provide network throughput and delay.

A secrecy aware relay selection method is proposed by Nomikos *et al*. [10] for 5G network communication. Based on the dissimilar relay aspects the communication characteristic such as protection range, establishing the channels, various access points, and capacity of the memory and processing, secrecy features are determined. For the proposed method the communication selection procedures is considered to achieve better secrecy rate. This method improved communication privacy with better power consumption and less delay.

Guan *et al*. [11] introduced group routing between-ness centrality (GRBC) for improving the security features of 5G communication networks. This method relies on software defined networks (SDN) achieving network function virtualization (NFV) at the time of interoperability. Placing secure security services are refined based on radio resource, security level, time delay as modeled as an integer linear programming. This optimal security placement method improves the security features of the network by retaining high level of survival nodes.

Cao *et al*. [12] proposed efficient group-based handover authentication (EGHR) protocol for improving the security features of 5G communication. EGHR is more specific in providing security for machine level interactions. EGHR improves the verification in overhead signaling and bandwidth depletion by the vigorous protection needs. The proposed protocol isprotectingamong the various attacks with better radio resource utilization and authentication.

A distributed denial of service (DDoS) attack detection is introduced by Mamolar *et al*. [13] for improving the reliability of multi-tenant overlay networks. This detection method exploits the advantages of intrusion detection system (IDS) that evades network traffic and security constraints in communication. This traversal based detection system improves the rate of security at infrastructure and user level concurrently. This IDS based detection system improves network performance by reducing delay and overhead.

In account of administering end-to-end security in 5G communication networks, Kotulski *et al*. [14] exploited the concepts of network slicing. Network segregation is presented as a part of management and orchestration architecture (MANO) that provides exceptional security features with adaptable and flexible security features assimilating the benefits of radio access networks and core networks.

Tao *et al*. [15] analyzed the secrecy and outage features of large scale cellular networks as a part of securing the future communication networks. The authors derive a closed form of explicit analysis for single-antenna systems based on Poisson distribution system. This system is advantageous in combating non-cooperative attacks and retaining physical layer security of the communication networks. Transmit antenna selection (TAS) employed by the authors is useful in determining secrecy rate by adapting secure communicating neighbors in the network. This method achieves less outage with better secrecy.

A. *Dynamic Access Control and Authentication Framework*

In this paper we design a history based access control and dynamic authentication framework for future 5G networks. The functions of the framework are designed to leverage security features of user equipment (UE) level communications. The user-level communications are authenticated to face anomalous access issues and security breaches.

B. *Network Model*

We consider a 5G network as illustrated in Fig. 1. The 5G architecture is segregated into three layers such as data, Access and user layers.

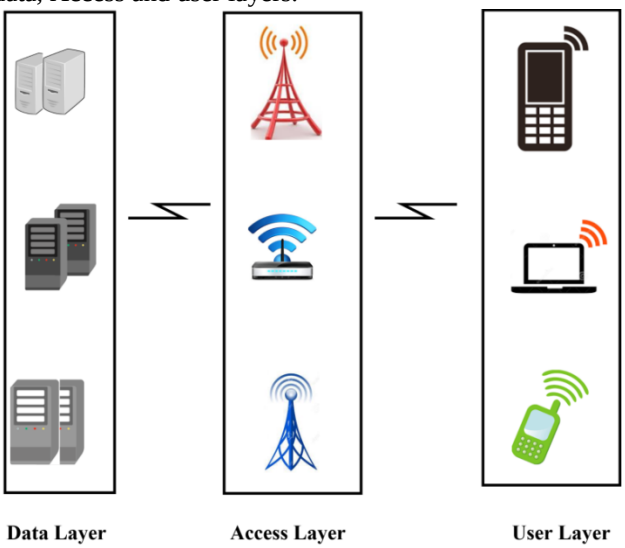

Fig. 1. Layered representation of 5G networks

Data Layer: encompasses multiple resources and service providers such as: data, file, multimedia and web, certificate authorities, communication and access policy servers and storages. Data layer is pervasive and is distributed.

Access Layer: In this layer, the wireless technologies that have evolved such as 3G, wireless LANs, long term evolution (LTE), etc. are enclosed to provide seamless communication support for end-users. This network provides interoperability and communication hand-over

features. Besides, this layer grants integration of different networks forming heterogeneous network scale.

User Layer: User equipment (UE) is populated in this plane to access data and information. The communications from this layer relies on the radio access technologies (RAT) provided by the access layer. The layers are connected through dedicated wireless communication links.

III. Methodology

The framework provides authentication and access layer of the 5G network environment. Access points interconnects UE and authentication server (AS) in the data layer. The authentication process starts with UE registration. The process of authentication is then forwarded using authentication keys for UE to generate secure communication sessions.

As mentioned before, history based access control is estimated for the communicating users in each interval. UE identifier, communication delay and outage history of an UE determines in reliability for communication. Let $p(UE)$ be the preference of an UE defined by $p(UE) = \{ID, d, \rho_o\}$ where d and ρ_o are the delay and outage probability of the UE. User layer possesses multiple set S of $p(UE)$ depending on the density of UE. Let S and S_d represent the communication session of the UE with AS such that two co-operative sessions $S \times S \rightarrow S_d$ for a random bi-linear pair of authentication elements a and b from each side. Now, the authentication parameters p_a are

$$p_a = \{p, g^x, r, s, ID, I\} \tag{1}$$

where, p is a prime number, g is a random generator, x is an arbitrary value $\in [0,1]$. r Represents and exponents of the random integers I such that

$$\left.\begin{array}{c} I = x|\rho(UE)| \\ r = g^x|p| \end{array}\right\} \tag{2}$$

Let h represent the hash function; $h: \{0,1\}^x$ for the session S_d. The user layer shares the list of $\rho(UE)$ to the AS for registration with ID as reference. Let Q_k be the private key for the UE as generated by the AS, given by

$$\left.\begin{array}{c} Q_k = (\alpha, \alpha_o) \\ where\ \alpha = s_1^x . s_2^{\gamma d}, s_1, s_2 \in S \\ \alpha_o = g^{xd} \\ \text{And } \gamma = {}^{r}/_{|p|} = g^x \end{array}\right\} \tag{3}$$

The generated Q_k is cross-checked by the UE for the consistency of $(g, \alpha) = g^{xd}\alpha_1$. Post the key generation process, the authentication hash string is generated as $h(msg, r)$ signed using Q_k. To secure the S, UE generates random slot integers ω_1, ω_2 and ω_3 as

$$\left.\begin{array}{c} \omega_1 = \alpha . g^{xd}\ (msg \prod_{i \in k} msg_i)^{s_1 \oplus s_2} \\ \omega_2 = g^{s_1 \oplus s_2} \\ \omega_3 = \alpha_o^d \end{array}\right\} \tag{4}$$

where k represents the bits to be exchanged from UE. With the generation of random slot integers for registration authentication and communication, the session key s_k is generated for securing S and d.

$$s_k = Q_k * Q_{AS}^* \tag{5}$$

where Q_{AS} represents the private key of the authentication server and

$$\left.\begin{array}{c} Q_{AS}^* = Q_{AS} * \omega_1 \\ Q_k^* = Q_k * \omega_2 \end{array}\right\} \tag{6}$$

ω_3 is used for the session that exceeds d in S. If a variation is sensed in the d or communicating Q_k, the authentication parameter list is updated and the outage probability ρ_o. Similarly, by framing the authentication parameters, the UE can be accepted or rejected at the initial communication stage. The authentication framework process is illustrated in Fig. 2.

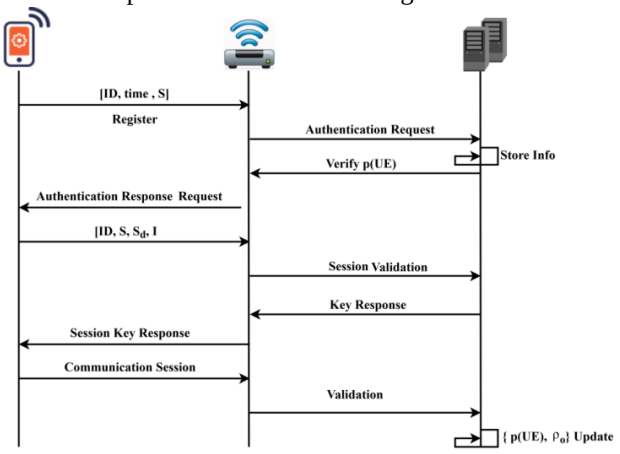

Fig. 2. Authentication framework process

A. Access Control

Communicating UE holds the information of $[ID, S, I, s_k]$ for a time interval d to satisfy the secrecy requirements. Valid user registration information is stored in AS and updated for all S_d. The ρ_o of a UE is estimated as

$$\rho_o = 1 - d\left\{\frac{s_1 s_2}{\rho(UE) + S.d}\right\} \tag{7}$$

The UE exceeds the next S to pursue communication such that $\prod s = S_d$

The AS on receiving the communication request in S, performs an attribute verification such that,

$$s_k = (\alpha, \alpha_o) = \left(\frac{1}{g^x}\right)\ (g)^{dr}, \left(g s_1, s_2, g^{xd}\frac{1}{g^{\frac{1}{\gamma}}}\right) \tag{8}$$

for all the UE communications in S. The difference in S_d varies the S_d as p_a is updated in $(S_d - S)$ variation. More specifically, the time difference in the communication session (i.e) d is computed using equation (9) as

$$d = \left(1 + \frac{1}{s^2}\right)\left(S - \frac{s_1}{|p|}\right) \tag{9}$$

In this d, based on p_a and ρ_o the process of communication is mutually authenticated by varying ω_3

instead of ω_1 andω_2. Therefore, the random factor ω_3 is modified as

$$\omega_3(s_k)_d = [\, s_2^d \, s_1(msg \prod_{i\in k} msg_i) \,, g^{s_1 \oplus s^2} \frac{1}{g}, r^d] \quad (10)$$

If a discrepancy occurs in d or access is delayed due to p_a , then communication is aborted. If the communication is aborted, then p_a is updated by discarding S for the specific ID. Therefore, the particular ID is suspended from communication until ρ_o(suspended ID) $< \rho_o(S)$. (i.e.,) the UE suspended from communication re-establishes communication until its outage observed in any d must be less than the previous outages in all S. The probability of estimating as in (10) occurs if the difference in slots (S and S_d) is high than the other UE. In this case, ω_3 for the less $\rho_o$is estimated to confine the impact of adversary UE so as to leverage the security rate. In this case, outage probability is decisive using continuous monitoring of the S_d. If a UE exceeds S, then a time stamp value is assigned. Therefore, the new time stamp is vails until the extended communication S. With the time stamp value, the session key is updated for two cases as discussed below.

Case 1: If the UE communicates with the same access layer terminal.

Solution1: The previously established s_k is extended with time stamp inclusion. Now, a define time stamp (t_s) is augmented for ω_3 alone such that a new I is generated for accommodating the change. The hash in this case is defined as $h(msg, r||t_s)$. To reduce the outage of the current communication t_s is set as a value $\in [S_d, S_{d+1}]$. Therefore, the authenticated message communication is initialized by ensuring verification of $h(msg, r||t_s) \forall\, S_d$. Here, the authentication credentials are shared between access layer units and UE in different communication slots with redefinedp_a. The disclosure of credentials is restricted between the communicating access points with S_d changes. If S_d and S_{d+1} exceeds t_s, then communication is pursued else the ρ_o of the UE is estimated for ω_1 and ω_2 jointly. The current UE is revoked from its access and is suspended from communication by de-allocationQ_k. The individual slots $s_1 \neq 0$ and$s_2 \rightarrow 0\ \forall t_s > (S_{d+1} - S_d)$.

Case 2: If the UE communicates with a new access layer units.

Solution 2: The probability of accepting the communication is high as the access layer unit considers the UE request as new. In this scenario, ω_1 , ω_2 are estimated for p_a and if s_k is extended for and S such that $\sum S = S_d$, then s_1 requires ω_1 and ω_2 where ω_3 relies on new s_1

(i.e.) the communication re-instigated for the existing UE. This is because the UE communication faces hand-over for the next S. Now, the value of (α, α_o) is randomly utilized such that

$$g^x = s_{k+1} = (g^x)^d and \quad (11)$$

The authentication hash is represented as $h(msg, h(msg, r||t_s).$, I) . In the successive communication slot, if S_d is required then, the session key is updated consenting d for ω_3 as in (10).

The advantages of this scenario is its latency less communication due to independent analysis of p_a and ρ_o for each Sor S_d, Therefore, the rate of authentication as exploited by p_a is autonomous of d for any communication level securing UE and reducing outage. Outage of the UE in its communication session is estimated for ensuring the participation of the access layer unit and seamless connectivity. This feature lets to permits accessible and less delay incurring communications. The designed framework provides both a complete security and independent access control in a dynamic manner.

IV. Performance Analysis

To evaluate the performance of the proposed dynamic authentication framework we introduce an eavesdropping adversary model as in [10]. The performance of the system is modeled using simulations and the corresponding simulation settings are presented in Table I.

TABLE I: Simulation Setting and Values

Simulation Setting	Value
Network Size	300m x 300m
UEs	150
Communication Slots	50
Eaves Droppers	4
Maximumρ_o	240ms

As a measure of assessing the performance of the proposed method, the experimental results are compared with the existing methods in [10] and [15]. The metrics considered for comparative analysis are security rate, secrecy rate, and outage probability and connection latency.

A. Security Rate Analysis

In Fig. 3, the security rate of the proposed method is compared with the existing methods in [10] and [15] respectively. Security rate is determined on the basis of transmitted bits at an average slot post authentication. Security provided in $s_1 \in S$ is accounted as the next session satisfiesS_d. Authentication provided in both the cases of access layer equipment assignment is considered in this security rate. The combined and individual security authentication provided is accounted for all UE satisfying (10). Besides, the updatedp_a in case 1 and case 2 for the varying arbitrary values augment to the security rate to reduce outage and improve the secrecy rate. These two features are balanced on the basis of the communication history possessed by the UE. Therefore,

authenticating the UE post registration initializes the security feature in communication.

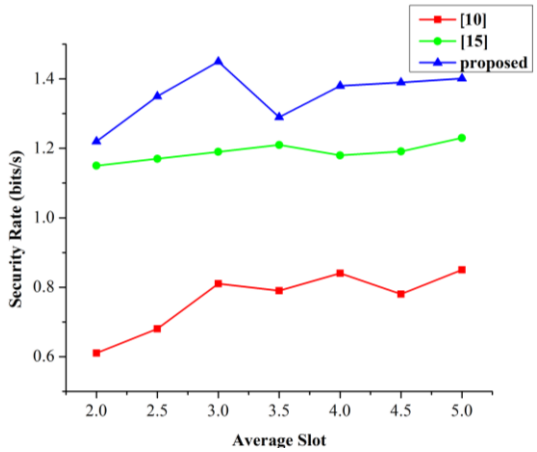

Fig. 3. Security rate analyses

B. Secrecy Rate Analysis

A comparative analysis of secrecy rate is presented in Fig. 4. In the proposed method, there are two levels of security i.e. a combined framework and an independent UE level framework. Authentication features of S and extendedS_d is determined usingp_a with the inclusion oft_s based on the random slot integers. The random slot integers are mapped across all communication slots for authentication, communication and access point change over or extended communication. This ensures non-discoverable amenity for the UE in both the communication sessions. Similarly, the random slot integers exploitω_1 andω_2 for a communication within S. On the other hand, if the communication is extended, then $\omega_3(s_k)_d$ determines the session key for communication. Hence in both the cases, the UE satisfying equation (10) andp_a attributes achieve better secrecy rate.

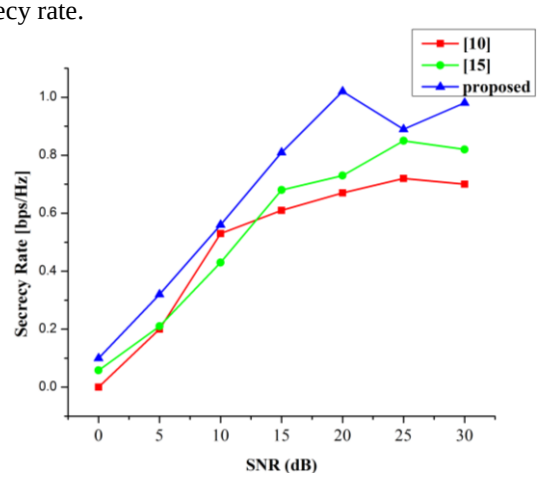

Fig. 4. Secrecy rate analyses

C. Outage Probability Analysis

Fig. 5 depicts outage probability comparison with respect to the secrecy factor. In the proposed framework, secrecy factor varies for the two cases explained with respect to the access layer communication attachment. Communication time difference across the allocated slots is estimated at the end of each session and is augmented as an estimation value. The outage as defined in (7) is estimated for the UE unsatisfying$s_1 \neq 0$.In this case, the outage causing UE is suspended from the communication until $s_2 \rightarrow 0\ \forall t_s > (S_{d+1} - S_d)$. The time delay in communication is verified for all messages that are authenticated as $h(msg, r||t_s) \forall S_d$. This helps to retain less outage UE in the communication process and hence retaining the secrecy factor with respect to d.

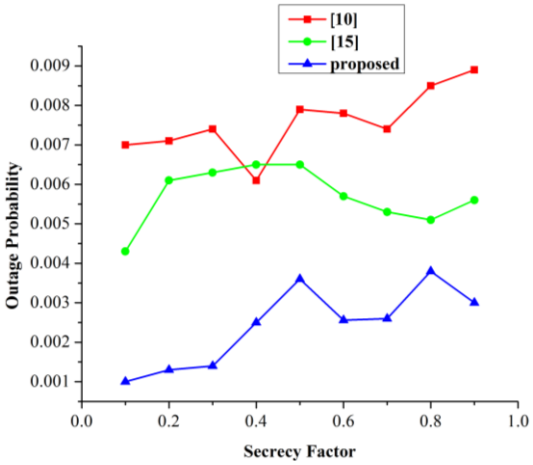

Fig. 5. Outage probability analyses

D. Connection Latency Analysis

UE communication is instigated post registration process and verification at two levels: with the conventional session key established and the session key established in S_d. Unlike the existing methods, communication request is processed based on the attributes and the history of the UE that requires less time. The reconnection time is high if the communication slot is less than the available UEs. In this case, the overflow UEs are assigned to another access layer device with the preference of $\omega_3(s_k)_d$ such that $t_s > (S_{d+1} - S_d)$. Authenticated used adapt the maximum time of$S_{d+1} - t_s$ for establishing connection that is comparatively less in the proposed method (Refer Fig. 6).Table II presents the comparative experimental values of the methods in [10], [15] and the proposed method.

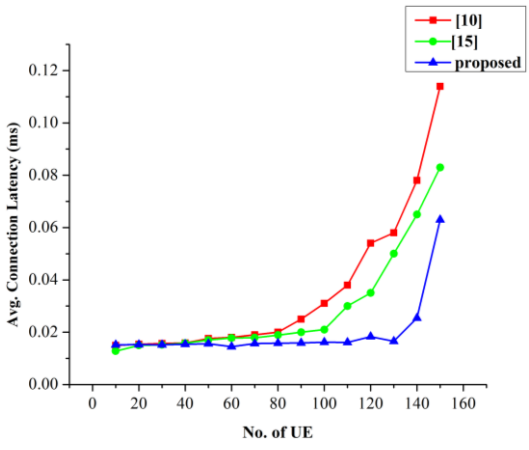

Fig. 6 Average Connection Latency Analyses

TABLE II: COMPARATIVE EXPERIMENTAL VALUES

Metrics	[10]	[15]	Proposed
Security Rate (bits/s)	0.85	1.15	1.22
Secrecy Rate (bps/Hz)	0.7	0.82	0.981
Outage Probability	0.0089	0.0056	0.003
Connection Latency (ms)	0.114	0.083	0.063

V. CONCLUSION

In this paper, we present a dynamic access control and authentication framework for securing 5G communication. The proposed framework operates in both integrated and independent manner for improving the rate of security through authentication. Communication authentication is administered using session keys that are dependent on the time stamp feature provided by the access layer devices. Similarly, the outage constraint UEs are prevented from accessing secure access layer components to reduce the impact of anomalies in communication by updating the parameters for each communication slot. Session key, outage analysis based authentication framework is extended for both individual security of the devices based on its attributes and integrated UEs based on slot parameters. These constructive features help to improve the security features of the network by improving security rate by 18.04%, secrecy rate by 22.53% and reducing outage by a factor of 0.43 and delay by 34.42% correspondingly.

CONFLICT OF INTEREST

The authors declare no conflict of interest

AUTHOR CONTRIBUTIONS

The contributions of the authors are such that Sakthibalan P proposed the ideology behind the research and carried forward the work with its implementation and presentation. Besides, Devarajan K scrutinized and verified the presentation through proofreading and technical assistance for the research ideology. Both the authors are satisfied with the final presentation.

REFERENCES

[1] G. Bianchi, E. Biton, N. Blefari-Melazzi, I. Borges, L. Chiaraviglio, P. D. L. C. Ramos, *et al*., "Superfluidity: a flexible functional architecture for 5G networks," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 9, pp. 1178–1186, 2016.

[2] L. Chiaraviglio, A. S. Cacciapuoti, G. D. Martino, M. Fiore, M. Montesano, D. Trucchi, and N. B. Melazzi, "Planning 5G networks under EMF constraints: State of the art and vision," *IEEE Access*, vol. 6, pp. 51021–51037, 2018.

[3] M. Agiwal, A. Roy, and N. Saxena, ''Next generation 5G wireless networks: A comprehensive survey,'' *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[4] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2659–2672, 2016.

[5] H. M. Wang and T. X. Zheng, "Physical layer security in heterogeneous cellular network," *Physical Layer Security in Random Cellular Networks SpringerBriefs in Computer Science*, pp. 61–84, 2016. .

[6] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[7] F. Tian, X. Chen, S. Liu, X. Yuan, D. Li, X. Zhang, and Z. Yang, "Secrecy rate optimization in wireless multi-hop full duplex networks," *IEEE Access*, vol. 6, pp. 5695–5704, 2018.

[8] L. Xiao, D. Jiang, D. Xu, H. Zhu, Y. Zhang, and H. V. Poor, "Two-Dimensional antijamming mobile communication based on reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9499–9512, 2018.

[9] L. F. Maimó, A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, and G. M. Pérez, "Dynamic management of a deep learning-based anomaly detection system for 5G networks," *Journal of Ambient Intelligence and Humanized Computing*, 2018.

[10] N. Nomikos, A. Nieto, P. Makris, D. N. Skoutas, D. Vouyioukas, P. Rizomiliotis, J. Lopez, and C. Skianis, "Relay selection for secure 5G green communications," *Telecommunication Systems*, vol. 59, no. 1, pp. 169–187, 2014.

[11] J. Guan, Z. Wei, and I. You, "GRBC-based Network Security Functions placement scheme in SDS for 5G security," *Journal of Network and Computer Applications*, vol. 114, pp. 48–56, 2018.

[12] J. Cao, M. Ma, H. Li, Y. Fu, and X. Liu, "EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks," *Journal of Network and Computer Applications*, vol. 102, pp. 1–16, 2018.

[13] A. S. Mamolar, Z. Pervez, J. M. A. Calero, and A. M. Khattak, "Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks," *Computers & Security*, vol. 79, pp. 132–147, 2018.

[14] Z. Kotulski, T. W. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J. P. Wary, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP Journal on Information Security*, vol. 2018, no. 1, 2018.

[15] L. Tao, W. Yang, Y. Cai, and D. Chen, "On secrecy outage probability and average secrecy rate of large-scale cellular networks," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–14, 2018.

Sakthibalan. P received his B.E. degree from A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu, India in 2006 and M.E. degree from Annamalai University, Chidambaram, Tamil Nadu, India, in 2010. He is currently working as Asst. Professor in the department of Electronics and Communication Engineering, Annamalai University, Chidambaram, Tamil Nadu, India and pursuing Ph.D. degree with the same department. His research interests include Wireless Systems and Communication Networks.

Dr. Devarajan. K received his B.E. degree from Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India in 2005 and M.E. degree from Annamalai University, Chidambaram, Tamil Nadu, India, in 2011. He also received his Doctorate degree from Annamalai University, Chidambaram, Tamil Nadu, India with the Department of Electronics and Communication Engineering, in 2017.He is currently working as Asst. Professor with the department of Electronics and Communication Engineering, Annamalai University, Chidambaram, Tamil Nadu, India. He has published 20 national and international journals. His research area includes mobile ad-hoc networks, Wireless Systems, Signal Processing and Communication Networks.