Towards Security and Privacy Preservation in 5G Networks

Vincent Omollo Nyangaresi[1]
Faculty of Biological & Physical Sciences
Tom Mboya University College
Homabay, Kenya.
vnyangaresi@tmuc.ac.ke
Zaid Ameen Abduljabbar[2]
Department of Computer Science
College of Education for Pure Sciences,
University of Basrah,
Basrah, Iraq.
Shenzhen Insitute of Huazhong University of Science & Technology,
Shenzhen, China.
zaid.ameen@uobasrah.edu.iq
Mustafa A. Al Sibahee[3]
Computer Technology Engineering Department,
Iraq University College,
Basrah, Iraq.
College of Big Data and Internet,
Shenzhen Technology University,
Shenzhen, China.
mustafa@sztu.edu.cn
Iman Qays Abduljaleel[4]
Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Iraq
iman.abduljaleel@uobasrah.edu.iq
Enas Wahab Abood[5]
Department of Mathemaitics, College of Science,
University of Basrah,
Basrah, Iraq.
enas.abood@uobasrah.edu.iq

2021 29th Telecommunications Forum (TELFOR) | 978-1-6654-2585-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/TELFOR52709.2021.9653385

***Abstract*— The Fifth Generation (5G) networks support various service delivery models such as Device to Device (D2D) communication, Unmanned Aerial Vehicles (UAVs) and Vehicular Ad Hoc Networks (VANETS) among others. In these networks, massive personal and private data items are being exchanged among numerous heterogeneous devices. As such, security and privacy leaks can have devastating repercussions. Many protocols have been presented for device authentication, starting with Authentication and Key Agreement (AKA) introduced by the Third-Generation Partnership Project (3GPP). Numerous attacks have been described against this AKA protocol and hence other schemes have been presented in literature. Although they address some of these security and privacy issues, some of these schemes are inefficient while others are still susceptible to other attacks. In this paper, a protocol that protects the exchanged packets against ephemeral leakages, man-in-the-middle, impersonation and offline guessing attacks is presented. In terms of bandwidth requirements and execution time, the proposed protocol had the lowest values among its peers.**

***Keywords*— 5G, attacks, bandwidth, authentication, execution time, privacy, security.**

I. INTRODUCTION

The 5G networks enhance the Quality of Service (QoS) in terms of extremely reliable and stable data transmissions, higher throughputs and ultra-low latencies. However, security and privacy are major issues in these networks. As explained in [1], attackers can easily eavesdrop or intercept the transmitted packets, as well as forge and modify them. The openness of the 5G environment, coupled with fast handovers has been identified in [2] as being the source of these security and privacy vulnerabilities. The transformation into an all-internet protocol (IP) network implies that these networks are susceptible to all known IP attacks. As such, upholding high levels of privacy and security is key for the successful deployments of 5G networks. The need to support numerous devices, offer better connectivity and higher data rates has led to the introduction of heterogeneous networks (HetNets). However, these HetNets introduce numerous security and privacy challenges [3] such as location privacy.

As explained in [4], 5G networks are characterized by massive roaming due to the existence of macro and micro operators. Because of their lightweight implementations, these macro and micro cells are susceptible to many threats and active attacks. In addition, the many 5G service delivery models such as Internet of Things (IoT) introduce numerous security and privacy vulnerabilities, owing to the increased attack surfaces. Consequently, security and privacy techniques in 5G should be efficient and flexible to suit these highly dynamic environments [5]. Authors in [6] explain that massive personal data flows over 5G networks, such as IoT platforms. There is therefore need for security services performance enhancements in these new use cases, in terms of exchanged overheads and latencies.

Although the Fourth Generation (4G) networks offer users and network operators some levels of security and reliability, new security and privacy solutions are required to support the new service delivery models, architectures and advanced technologies supported by 5G networks [7]. In this regard, most of the conventional security protocols are not ideal for these service delivery models, especially IoT where most of the devices are resource constrained [8]. This is due to their high computation, storage and communication overheads. In addition, these schemes rarely take into consideration the heterogeneity of the supported IoT devices. As such, attacks such as main-in-the-middle (MitM) have continued to wreck havoc in 5G networks [9]. In addition, authors in [10] identify authentication of communicating entities before the establishment of secure channels as being an open challenge for the preservation of confidentiality and integrity. Consequently, novel security architectures are required to offer flexible privacy and security solutions that are geared towards high QoS provisioning [5]. The contributions of this paper are as follows:

I. A pseudonym-based authentication protocol is developed for 5G network elements.
II. Informal security analysis shows that this protocol is resilient against ephemeral leakages, MitM, impersonation and offline guessing attacks.
III. Performance evaluation shows that this protocol exhibits the lowest execution time and has the least bandwidth requirements among its peers.

The rest of this paper is organized as follows: Section II presents related work while Section III discusses the system model of the proposed protocol. Section IV presents security

978-1-6654-2585-8/21/$31.00 ©2021 IEEE

and comparative analysis while Section V concludes the paper and provides future work.

II. RELATED WORK

Privacy and security of the packets exchanged over the 5G networks is critical, and hence researchers have presented many security solutions in literature. For instance, 3GPP has introduced AKA technique in 4G and 5G networks. However, this AKA protocol is inadequate for the management of the vast 5G network devices [11]. In addition, attacks such as Denial of Service (DoS), user identity disclosure, MitM and impersonation are still possible in 5G networks [12]. To curb these attacks, an identity-based authentication protocol is presented in [13]. However, this scheme is still susceptible to impersonation attacks. A neuro-fuzzy security technique is developed in [14], in which elliptic curve cryptography (ECC) is deployed to authenticate the IoT devices. However, this technique has high computation complexity. On the other hand, two blockchain based authentication protocols are presented in [15] and [16]. However, the scheme in [15] experiences high computation overheads at high traffic levels while the scheme in [16] has high storage and computational complexities. Similarly, the protocol in [17] has high computational complexity.

Although the authentication scheme in [18] provides resilience against MitM and linkability, it employs public keys which lead to high latencies [19]. On the other hand, a group authentication protocol has been introduced in [20]. Unfortunately, malicious group members or group leader may leak group members' data [21] or lead to the tracking of the group members [22]. The AKA protocol presented in [23] has high computation and communication costs while the scheme in [24] is vulnerable to DoS and MitM attacks.

III. SYSTEM MODEL

The entities involved in the proposed authentication and key agreement procedures includes the Anchor Mobility Function (AMF), new radio Node B (gNB), User Equipment (EU) and the subscriber (SB) as shown in Fig.1.

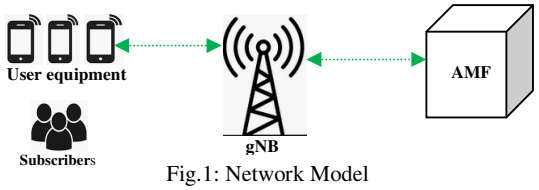

Fig.1: Network Model

The detailed description of these network components can be found in [6].Table 1 presents the symbols deployed in this paper. The proposed protocol consisted of the initialization phase, authentication and key agreement.

TABLE 1: DEPLOYED SYMBOLS

Symbol	Description
$\wp$	AMF master key
ID_{UE}	UE unique identity
ID_{gNB}	gNB unique identity
SK_{UE}	UE's secret key
$\mathbb{N}_i$	Random nonces
$\underline{Z}$	Session key
h(.)	One way hashing operation
$\|$	Concatenation operation
$\oplus$	XOR operation

A. Initialization phase

In this phase, the AMF generates master key $\wp$, UE unique identity ID_{UE} and gNB unique identity ID_{gNB}. In addition, the AMF assigns the UE some secret key SK_{UE}. The following steps are then executed during this phase:

Step 1: The UE generates nonce $\mathbb{N}_1$ and derives $A=h(ID_{UE}\|\mathbb{N}_1)$. It then composes $\Gamma_1=\{A, \mathbb{N}_1\}$ and transmits it to the AMF through some secure channels.

Step 2: On receiving Γ_1, the AMF generates nonce $\mathbb{N}_2$ before deriving $B=h(A\|\wp\|\mathbb{N}_2)$. Afterwards, the AMF composes $\Gamma_2=\{A, B, \mathbb{N}_1\}$ and sends it to the gNB through a secure channel. In addition, it transmits security parameter {B} to the UE via secure channels before publishing security parameter {A}.

Step 3: Upon receipt of {A}, the UE derives $X_1=\mathbb{N}_1\oplus h(ID_{UE}\|SK_{UE})$ and $X_2=B\oplus h(\mathbb{N}_1\|SK_{UE})$. Thereafter, it stores parameters $\{X_1, X_2, A\}$ in its memory.

Step 4: For the SB to effectively access the 5G core network services, identity ID_U and password P_U are selected before generating nonce $\mathbb{N}_3$. Thereafter, security parameter $C_U=h(ID_U\|\mathbb{N}_3)$ is computed before being sent to the AMF via some secure channels.

Step 5: On receiving C_U, the AMF computes $D_1=h(C_U\|\wp\|\mathbb{N}_2)$ and $D_2=h(C_U\|D_1)$. It then constructs $\Gamma_3=\{C_U, D_2, D_1\}$ before sending it to the gNB through a secure channel. It also composes $\Gamma_4=\{D_1, D_2\}$ and sends it to the SB.

Step 6: Upon receiving Γ_4, the SB computes $E_1=h(P_U\|\mathbb{N}_3)$, $E_2=\mathbb{N}_3\oplus h(ID_U\|P_U)$,$E_3=h(ID_U\|P_U\|\mathbb{N}_3\|E_1)$,$E_4=D_2\oplus h(\mathbb{N}_3\|E_1)$ and $E_5=D_1\oplus h(D_2\|E_1)$. Thereafter, the computed SB security tokens $\{E_2, E_3, E_4, E_5, C_U\}$ are stored in the UE's memory.

B. Authentication and Key Agreement Phase

During the mutual authentication and key agreement phase, the following steps are executed.

Step 1: The SB supplies the pair $\{ID_U, P_U\}$ to the UE which then derives the following parameters:

$\mathbb{N}_3=E_2\oplus h(ID_U\|P_U)$
$E_1=h(P_U\|\mathbb{N}_3)$ and
$E_3^*=h(ID_U\|P_U\|\mathbb{N}_3\|E_1)$

Thereafter, it checks whether $E_3^*=E_3$ and if it is not, the session is aborted. However, if this verification is successful, the UE generates nonce $\mathbb{N}_4$ before computing:

$D_2=E_4\oplus h(\mathbb{N}_3\|E_1)$
$D_1=E_5\oplus h(D_2\|E_1)$
$Q_1=h(C_U\|D_2\|D_1)\oplus(\mathbb{N}_4\|A)$
$R_1=h(ID_U\|\mathbb{N}_4)\oplus h(D_1\|\mathbb{N}_4)$
$\ddot{Y}_1=h(C_U\|D_2\|\mathbb{N}_4\|A\|D_1)$

It then constructs $\Gamma_5=\{C_U, Q_1, R_1, \ddot{Y}_1\}$ and sends it to gNB over public channels.

Step 2: On receiving Γ_5, the gNB retrieves D_2 and D_1 corresponding to the received C_U in Γ_5. This is followed by the derivation of the following:

$(\mathbb{N}_4^*\|A^*)=Q_1\oplus h(C_U\|D_2\|D_1)$
$\ddot{Y}_1^*=h(C_U\|D_2\|\mathbb{N}_4^*\|A^*\|D_1)$

Next, it checks whether $\ddot{Y}_1^*=\ddot{Y}_1$ and if this condition is false, the authentication session is terminated. However, if the verification is successful, gNB retrieves *B* and $\mathbb{N}_1$ corresponding to *A*. Thereafter, the gNB generates nonce $\mathbb{N}_5$ before computing the following security parameters:

$Q_2=h(\mathbb{N}_4\|\mathbb{N}_5)$
$Q_3=h(A\|B\|\mathbb{N}_1)\oplus Q_2$
$h(ID_U\|\mathbb{N}_4)=R_1\oplus h(D_1\|\mathbb{N}_4)$
$R_2=(h(ID_U\|\mathbb{N}_4)\|h(ID_{gNB}\|\mathbb{N}_5))\oplus h(B\|\mathbb{N}_1)$

$\ddot{Y}_2=h(C_U||Q_2||B)$

It then composes authentication token $\Gamma_6=\{C_U, Q_3, R_2, \ddot{Y}_2\}$ and transmits it to the UE.

Step 3: When the UE receives Γ_6, it derives the following:

$\mathbb{N}_1=X_1 \oplus h(ID_{UE}||SK_{UE})$

$B=X_2 \oplus h(\mathbb{N}_1||SK_{UE})$

$Q_2^*=Q_3 \oplus h(A||B||\mathbb{N}_1)$

$\ddot{Y}_2^*=h(C_U||Q_2^*||B)$

This is followed by the confirmation of whether $\ddot{Y}_2^*=\ddot{Y}_2$, and if this condition does not hold, the authentication session is aborted. However, if it holds, the UE generates nonce $\mathbb{N}_6$ before calculating the following parameters:

$(h(ID_U||\mathbb{N}_4)||h(ID_{gNB}||\mathbb{N}_5))=R_2 \oplus h(B||\mathbb{N}_1)$

$\underline{Z}=h(h(ID_U||\mathbb{N}_4)||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6))$

$Q_4=h(A||B||\mathbb{N}_1) \oplus h(ID_{UE}||\mathbb{N}_6)$,

$F_1=h(C_U||A||Q_2^*||h(ID_{UE}||\mathbb{N}_6||B)$

Finally, it constructs $\Gamma_7=\{Q_4, F_1\}$ and sends it to the gNB.

Step 4: Upon receipt of Γ_7, the gNB derives $h(ID_{UE}||\mathbb{N}_6)=Q_4 \oplus h(A||B||\mathbb{N}_1)$ and $F_1^*=h(C_U||A||Q_2||h(ID_{UE}||\mathbb{N}_6||B)$. It then checks whether $F_1^*=F_1$ and if it is not, the session is aborted, otherwise it proceeds to compute the following parameters:

$\underline{Z}=h(h(ID_U||\mathbb{N}_4)||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6))$

$C_U^{**}=h(C_U||\mathbb{N}_4), D_2^*=h(C_U^{**}||D_1)$

$Q_5=h(D_2||\mathbb{N}_4) \oplus (h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6)||C_U^{**})$

$F_2=h(C_U||\mathbb{N}_4||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6)||C_U^{**}||D_1)$

The gNB buffers $\{C_U, D_2\}$ together with $\{C_U^{**}, D_2^*\}$ in its database. Finally it constructs $\Gamma_8=\{Q_5, F_2\}$ and transmits it to the UE.

Step 5: Once the UE receives Γ_8, it derives the following:

$C_U^{**}=h(C_U||\mathbb{N}_4)$

$(h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6||C_U^{**})= Q_5 \oplus h(D_2||\mathbb{N}_4)$

$F_2^*=h(C_U||\mathbb{N}_4||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6)||C_U^{**}||D_1)$

Thereafter, it verifies whether $F_2^*=F_2$ and if it is not, the session is terminated, otherwise it calculates the following parameter:

$\underline{Z}=h(h(ID_U||\mathbb{N}_4)||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6))$

Afterwards, it executes the following updates: $D_2^*=h(C_U^{**}||D_1)$, $E_4^*=D_2^* \oplus h(\mathbb{N}_3||E_1)$ and $E_5^*=D_1 \oplus h(D_2^*||E_1)$. Next, it substitutes $\{E_4, E_5, C_U\}$ with $\{E_4^*, E_5^*, C_U^{**}\}$ in its database. Finally, it computes $Q_6=h(\underline{Z}||C_U^{**})$ before sending it to the gNB.

Step 6: Upon receiving Q_6, the gNB re-computes $Q_6^*=h(\underline{Z}||C_U^{**})$ and validates whether $Q_6^*=Q_6$ holds and if it is not, the session is terminated. However, if this condition holds, the gNB erases $\{C_U, D_2\}$ from its repository.

IV. SECURITY AND COMPARATIVE ANALYSIS

This section presents the security as well as the performance evaluations of the proposed protocol. For security analysis, the most common 5G attacks vectors are deployed. However, for performance evaluation, execution time and bandwidth requirements are utilized.

A. Security Evaluation

In this sub-section, it is shown that the proposed protocol offers anonymity, mutual authentication, untraceability, forward key secrecy, and is resilient against MitM, impersonation, ephemeral disclosure and offline guessing attacks.

Forward key secrecy: suppose that an attacker has knowledge of long term keys $\{\wp, D_1, B, SK_{UE}\}$. An attempt is then made to derive the following session key:

$\underline{Z}^{New}=h(h(ID_U||\mathbb{N}_4)||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6))$

However, this session key incorporates nonces $\mathbb{N}_4$, $\mathbb{N}_5$ and $\mathbb{N}_6$ which are refreshed after every authentication session. As such, it is not possible to derive subsequent authentication session key $\underline{Z}^{New}$ based on the current session key.

Offline Guessing Attacks: In this attack, it is assumed that an attacker has physically captured the UE and extracted $E_2=\mathbb{N}_3 \oplus h(ID_U||P_U), E_3=h(ID_U||P_U||\mathbb{N}_3||E_1), E_4=D_2 \oplus h(\mathbb{N}_3||E_1)$ and $E_5=D_1 \oplus h(D_2||E_1)$ through power analysis. The goal is to use these parameters to compromise the security of the entire system. However, hashing is performed on the contents of these parameters and it is computationally infeasible to reverse it. Consequently, this attack fails.

Impersonation attacks: the assumption made in this attack is that an attacker can physically capture and extract secrets $\{E_2, E_3, E_4, E_5, C_U\}$. Thereafter, an attempt is made to intercept and modify exchanged messages over the public channel so as to impersonate the SB using message $\Gamma_5=\{C_U, Q_1, R_1, \ddot{Y}_1\}$. However, these parameters require the derivation of $\{E_1, D_2, D_1\}$ which require knowledge of ID_U, P_U and $\mathbb{N}_4$. As such, SB impersonation fails.

Strong mutual authentication: in the proposed protocol, all the communicating entities validate the messages received before trusting their contents. For instance, the SB authenticates the gNB using F_2^* and F_2, while the gNB authenticates the UE using $\{Q_6^*, \ddot{Y}_1^*, \ddot{Y}_1, Q_6\}$. On the other hand, the UE authenticates the SB using E_3^* and E_3. Similarly, the UE authenticates the gNB using $\ddot{Y}_2^*$ and $\ddot{Y}_2$.

Ephemeral leakage attacks: the assumption made here is that an attacker can intercept and capture session specific nonces $\{\mathbb{N}_4, \mathbb{N}_5, \mathbb{N}_6\}$. Thereafter, the adversary tries to compute the session key:

$\underline{Z}=h(h(ID_U||\mathbb{N}_4)||h(ID_{gNB}||\mathbb{N}_5)||h(ID_{UE}||\mathbb{N}_6))$

However, $\underline{Z}$ incorporates additional parameters such as the real identities of the SB, gNB and UE. Since all these parameters are unavailable to the adversary, this attack cannot materialize.

Replay and MitM attacks: Suppose that an attacker had intercepted exchanged messages during the previous authentication session and is interested in masquerading as the legitimate SB by sending $\{C_U, Q_1, R_1, \ddot{Y}_1\}$ to the gNB. However, since the gNB executes some freshness checks using $\mathbb{N}_4$ in $\ddot{Y}_1^*$ and $\mathbb{N}_4^*$ in $\ddot{Y}_1$, this replay is easily detected. Even if an adversary tries to modify $\Gamma_5=\{C_U, Q_1, R_1, \ddot{Y}_1\}$, parameters $\{Q_1, R_1, \ddot{Y}_1\}$ cannot be modified devoid of ID_U, P_U, $\mathbb{N}_4$ and shared secret D_1.

Untraceability and anonymity: The assumption made here is that an attacker is capable of intercepting the exchanged messages during the authentication and key agreement phase. The goal here is to associate these captured messages to some particular communicating entity. However, in the proposed protocol, the device real identities cannot be captured due to their masking in nonces $\mathbb{N}_3$, $\mathbb{N}_5$, and $\mathbb{N}_1$. In addition, after every successful authentication, the current session security parameters are refreshed. For instance, $\{E_4, E_5, C_U\}$ is substituted with $\{E_4^*, E_5^*, C_U^{**}\}$ in the UE's database. As such, the exchanged messages are stochastic and hence both anonymity and untraceability are upheld.

B. Performance evaluation

Execution time and bandwidth are the most widely deployed metrics for assessing performance of authentication protocols. As such, they are deployed to evaluate the proposed protocol.

***Execution Time*:** During the AKA phase, the proposed protocol executed a total of 42 hashing operations at the UE and gNB sides. Based on the values in [25], a single hashing

operation takes 5ms and as such, the total execution time for the proposed protocol is 210 ms. On the other hand, the schemes in [23], [13], [18] and [24] take 1230 ms, 1570 ms, 1020 ms and 780 ms respectively, as shown in Fig.2.

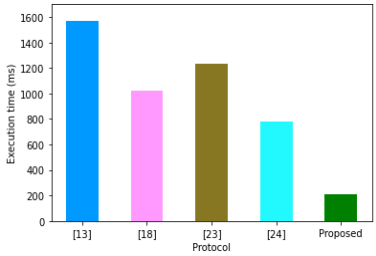

Fig.2: Execution Time Comparisons

It is evident from Fig.2 that the proposed protocol has the lowest execution time, and hence is the most ideal for 5G IoT devices.

***Bandwidth requirements*:** in the proposed protocol, the exchanged messages include Γ_5, Γ_6, Γ_7, Γ_8 and Q_6. Using the values in [25], symmetric key size, timestamps, identities, pseudo-random numbers, hashing, random numbers and MAC are 16 bytes, 5 bytes, 2 bytes, 32 bytes, 8 bytes, 16 bytes and 8 bytes respectively. Communication cost is derived as follows:

Γ_5={C_U= Q_1= R_1= $\ddot{Y}_1$=8}=32 bytes

Γ_6= {C_U= Q_3=R_2=$\ddot{Y}_2$}=32 bytes

Γ_7= {Q_4=F_1=8}= 16 bytes

Γ_8={Q_5=F_2=8}=16 bytes

Q_6=8 bytes

As such, the total communication overhead is 104 bytes. On the other hand, the bandwidth requirements for the scheme in [23], [13], [18] and [24] are 976 bytes, 496 bytes, 490 bytes and 576 bytes respectively, as shown in Fig.3.

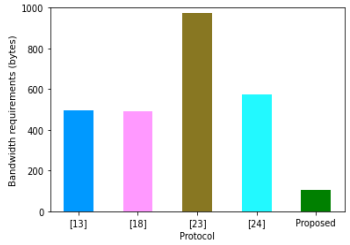

Fig.3: Bandwidth Requirements Comparisons

Based on Fig.3, the proposed protocol has the least bandwidth requirements, and hence is the most suitable for 5G's ultra-dense deployments where bandwidth preservation is critical.

V. Conclusion and Future Work

The goal of this paper included the development of a 5G authentication and key agreement protocol to address the security and performance issues inherent in conventional AKA protocols. The security evaluation has shown that this protocol offers mutual authentication, anonymity, forward key secrecy and untraceability. In addition, it is robust against impersonations, MitM, offline guessing and ephemeral disclosure attacks. In terms of performance, it has been shown to have the least execution time and bandwidth requirements. These features render it applicable in 5G service delivery models such as D2D and IoT where the communicating entities are resource constrained. Future work lies in the formal verification of the security features provided by this protocol.

References

[1] Z. Zhang, W. Zhang, Z. Qin, S. Hu, Z. Qian, and X. Chen, "A Secure Channel Established by the PF-CL-AKA Protocol with Two-Way ID-based Authentication in Advance for the 5G-based Wireless Mobile Network," in 2021 IEEE Asia Conference on Information Engineering (ACIE), 11-15, IEEE, 2021.

[2] N. Panwar, S. Sharma, and A.K. Singh, "A survey on 5G: The next generation of mobile communication," Physical Communication, 18, 64–84, 2016.

[3] V.O. Nyangaresi, A.J. Rodrigues,and S.O. Abeka, "ANN-FL secure handover protocol for 5G and beyond networks," in International Conference on e-Infrastructure and e-Services for Developing Countries, 99-118, Springer, Cham, 2020.

[4] P. Ahokangas, M. Matinmikko-Blue, S. Yrjölä, V. Seppänen, H. Hämmäinen, R. Jurva, and M. Latva-Aho, "Business models for local 5G micro operators," IEEE Trans. Cognit. Commun. Netw., 5(3), 730-740, 2019.

[5] D. Fang, and Y. Qian, "5G wireless security and privacy: Architecture and flexible mechanisms," IEEE Vehicular Technology Magazine, 15(2), 58-64, 2020.

[6] V.O. Nyangaresi, A.J. Rodrigues, and S.O. Abeka, "Efficient Group Authentication Protocol for Secure 5G Enabled Vehicular Communications," in 2020 16th International Computer Engineering Conference (ICENCO), 25-30, IEEE, 2020.

[7] D. Fang, Y. Qian, and R. Q. Hu, "Security requirement and standards for 4G and 5G wireless systems," GetMobile: Mobile Comput. Commun., 21(1), 15–20, 2018.

[8] V.O. Nyangaresi, "ECC Based Authentication Scheme for Smart Homes," in 2021 International Symposium ELMAR, 5-10, IEEE, 2021.

[9] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Communications Surveys & Tutorials, 18(3), 2027–2051, 2016.

[10] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," IEEE Access, 6, 18209–18237, 2018.

[11] M. Ouaissa, M. Houmer, and M. Ouaissa, "An enhanced authentication protocol based group for vehicular communications over 5G networks," in 2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet), 1-8, IEEE, 2020.

[12] V.O. Nyangaresi, A.J. Rodrigues, and S.O. Abeka, "Neuro-Fuzzy Based Handover Authentication Protocol for Ultra Dense 5G Networks," in 2020 2nd Global Power, Energy and Communication Conference (GPECOM), 339-344, IEEE, 2020.

[13] I. Gharsallah, S. Smaoui, and F. Zarai, "A secure efficient and lightweight authentication protocol for 5G cellular networks: Sel-aka," in 2019 15th International Wireless Communications Mobile Computing Conference, 1311–1316, 2019.

[14] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," IEEE Access, 7, 99573-99588, 2019.

[15] A. Yazdinejad, R.M. Parizi, A. Dehghantanha, and K.K. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," Computers & Security, 88, 101629, 2020.

[16] A.V. Rivera, A. Refaey, and E. Hossain, "A blockchain framework for secure task sharing in multi-access edge computing," IEEE Network, 35(3), 176-183, 2020.

[17] P. Krishnan, S. Duttagupta, and K. Achuthan, "VARMAN: Multiplane security framework for software defined networks," Computer Communications, 148, 215-239, 2019.

[18] F. Liu, J. Peng, and M. Zuo, "Toward a secure access to 5G network," in 2018 17th IEEE international conference on trust, security and privacy in computing and communications/ 12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), IEEE, 1121–1128, 2018.

[19] V.O Nyangaresi, and Z. Mohammad, "Privacy Preservation Protocol for Smart Grid Networks," in 2021 International Telecommunications Conference (ITC-Egypt), 1-4, IEEE, 2021.

[20] I. Alawe, Y. Hadjadj-Aoul, A. Ksentini, P. Bertin, and D. Darche, "On the scalability of 5g core network: the amf case," in 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 1-6, IEEE, 2018.

[21] G. Fortino, F. Messina, D. Rosaci, and G.M. Sarne, "Using blockchain in a reputation-based model for grouping agents in the internet of things," IEEE Transactions on Engineering Management, 67(4), 1231-1243, 2019.

[22] V.O. Nyangaresi, A.J. Rodrigues, and N.K. Taha, "Mutual Authentication Protocol for Secure VANET Data Exchanges," in International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, 58-76, Springer, Cham, 2021.

[23] A. Koutsos, "The 5G-AKA authentication protocol privacy," in 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 464–479, IEEE, 2019.

[24] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks," IEEE Access, 7, 64040–64052, 2019.

[25] Z. Haddad, M.M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based authentication for 5G networks," in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), IEEE, 189-194, 2020.