6th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November. 17-18, 2021

A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks

Vincent Omollo Nyangaresi
Tom Mboya University College, Faculty of Biological and Physical Sciences
199-40300, Homabay, Kenya
vnyangaresi@tmuc.ac.ke

ABSTRACT

The 5G mmWave networks support massive number of devices and offer salient features such as very low communication latencies and high signal stability. This has seen these networks being deployed to support various service delivery models such as device to device communication (D2D) and internet of things (IoT). Owing to the broadcast nature of the communication process in these models, security and privacy are major challenges in these heterogeneous networks. Although many protocols have been presented to curb these issues, they are not entirely effective in terms of performance and security. In this paper, a scheme is presented for authenticating the network entities before the initialization of packet exchange process. The formal verification of the protocol shows that it successfully establishes a session key between the communicating entities, executes freshness checks and verifies the sources of all exchanged messages. In doing so, it potentially thwarts packet replays and session hijacking attacks.

KEYWORDS: 5G, attacks, authentication, formal, mmWave, privacy, security, verification.

1 INTRODUCTION

The Fifth Generation Heterogeneous Networks (5G HetNets) offer enhancements on the quality of services (QoS), exampled by ultra-low latencies, more signal stability, increased reliability and higher throughputs. This has seen the developments of numerous service delivery models that are deploying 5G HetNets as the backbone. As explained in [1], 5G HetNets support ultra-reliable low latency communication (uRLLC), enhanced mobile broadband (eMBB) and massive machine-type communication (mMTC). However, the traffic channels in these networks are vulnerable to attacks such as message interception, forgery, eavesdropping and bogus packet injections [2], [3]. The novel architectures and advanced technologies that are continuously being incorporated in 5G HetNets to support various use cases inadvertently introduce new security, privacy and performance issues [4]. Other issues raised by these new technologies include transparency, decentralization and interoperability [5]. Owing to massive personal data being passed across these HetNets, privacy has also become a serious issue [6].

Structurally, security and privacy issues in 5G HetNets centres around subscribers, core network and access network [7]. At the core of the 5G network are session management function (SMF), authentication server function (AUSF), security anchor function (SEAF), and access and mobility management function (AMF). Whereas the AUSF executes user equipment (UE) authentication, SEAF boosts security at the network level by offering flexible authorization and authentication. It can introduce flexibility in the deployment of both AMF and SMF. Typically, data session setup and control is decoupled from device access authentication. In addition, extensible authentication protocol (EAP) is utilized to enhance authentication in 5G HetNets so that both Third Generation Partnership Project (3GPP) and non-3GPP access networks are supported.

Encryption schemes are normally utilized for masking the subscriber permanent identifier (SUPI). Doing this offers protection against subscriber data leakages during the initial stages. As such, SUPI offers both device and subscriber privacy protection, unlike in long term evolution (LTE) networks where the international mobile subscriber identity (IMSI) is sent in plaintext over the air interface. As explained in [8], 5G incorporates asymmetric encryption algorithms to protect the IMSI. Since SUPI is transmitted in enciphered form over the radio interfaces, tracking and spoofing attacks are prevented. Unfortunately, the limited bandwidth coupled with the broadcast nature of these networks render it cumbersome to totally eliminate attacks against integrity, confidentiality, privacy and authentication. Although LTE networks offer enhanced security and trust levels for both the network operators and subscribers, new security and privacy protocols are needed to support 5G network's advanced technologies, new architecture, performance and privacy requirements [9].

To achieve this, three authentication protocols are specified by 3GPP group. These techniques include 5G authentication and agreement (5G-AKA), Extensible Authentication Protocol AKA (EAP-AKA) and EAP transport layer security (EAP-TLS). Here, an ideal option is selected by the home network based on the correct identification of the subscriber using initialization protocol. Unfortunately, these protocols are still susceptible to a number of attacks [10]. In addition, authors in [11] explain that proper authentication of the 5G HetNets entities before the establishment of secure channels is still an open challenge. As such, novel architectures, and flexible security and privacy techniques are required to offer satisfactory protection at high performance levels [4]. The main contributions of this paper include the following:

- A novel security and privacy preserving technique is presented to authenticate users before the initialization of packet exchanges.
- It is shown that the proposed protocol upholds verification of the sources of the exchanged messages, executes freshness checks of the exchanged beacons and also establishes trust among the communicating entities
- Formal security analysis shows that the proposed protocol establishes a session key between the UE and the gNB to secure their data.

The rest of this paper is organized as follows: Section II discusses some past research in this domain while section III presents the proposed protocol. On the other hand, Section IV offers the security analysis of the proposed protocol while Section IV concludes the paper and gives future directions.

2 RELATED WORK

The AKA protocol has been standardized by 3GPP for authenticating entities in 5G networks. However, this protocol and its related schemes such as EAP-AKA and EAP-TLS are still vulnerable to attacks such as privacy leaks, packet replays, black hole, man-in-the-middle (MitM), denial of service (DoS) and entities impersonations [12],[10],[3]. In addition, authors in [13] explain that the conventional 5G AKA may not effectively fulfil security requirements in ultra-dense networks at low latencies and computational overheads. On the other hand, it is explained in [14] that the conventional 5G AKA protocols are not effective in handling many devices. As such, many schemes have been introduced to address some of these issues. For instance, a linear homomorphic signature based scheme is introduced in [15] for user authentication. However, the computation costs of this protocol is still high for resource constrained internet of things (IoT) devices [16] supported by 5G networks.

On the other hand, a deep Q-learning approach is presented in [17]. However, this approach fails to consider trust features of software defined networking (SDN) controllers blockchain. Authors in [18] have presented a game theory based scheme that is shown to be resilient against malicious discovery and directional antenna attacks. However, game theory is time consuming and hence the scheme has high computation costs. On the other hand, the security approach presented in [19] for 5G smart cities fails to validate the packet header and may lead to flow overloading attacks. In addition, the blockchain based SDN authentication protocol in [20] results in extremely high computation overheads at high traffic levels.

Similarly, the SDN-based hybrid security algorithm developed in [21] has high computation complexity. Moreover, the group-based AKA schemes that follow EPS-AKA framework have been introduced [22]. However, malicious group members and group leaders may compromise the entire network [23] security and privacy.

3 PROPOSED PROTOCOL

Although 3GPP's AKA protocols have been deployed for authenticating 5G entities, 3GPP failed to specify how to execute authentication in scenarios where a device requires access to another network slice [24]. In such a situation, the basic technique is for the core network to authenticate the devices again. In this section, a protocol that offers a straightforward handover authentication of the UE by the core network is presented. Table 1 presents the symbols used in this article, including their brief descriptions.

Table 1: Symbols and their Descriptions

Symbol	Description
p	A large prime number
E_p	Non-singular elliptic curve
Z_p	Prime finite field
P	Base point of order m over E_p
$\bar{I}$	Zero point or point at infinity
PK_A	AMF's private key
PUK_A	AMF's public key
h(.)	Collision resistant one-way hash function
Ǥ	Probabilistic generation function
Dz	Authentication deterministic function
β	User biometric data
Ľ	Biometric key length
$ꞵ_i$	Public reproduction parameter
H_D	Hamming distance
$\bar{y}$	Error tolerance threshold value
ID_{gNB}	gNB unique identity
$Ħ_{PR}$	gNB's private key
$Ħ_{PU}$	gNB's public key
Ψ_{PR}	UE's private key
Ψ_{PU}	UE's public key
τ_i	Timestamps
$\Delta\tau$	Threshold permitted transmission delays
g	Session key between UE and gNB
Reg_{Req}	Registration request
$\|\|$	Concatenation operation
$\oplus$	XOR operation

This protocol is decomposed into two major phases, namely system setup and AKA process as discussed below.

3.1 System setup phase

This phase is employed to initialize the security parameters that are used in the later AKA procedures. It is executed in five major steps as elaborated below.

Step 1: The AMF selects E_p over Z_p, followed by the selection of P such that m.P=$\bar{I}$. Next, the AMF chooses its private key PK_A before computing the equivalent public key PUK_A = PK_A.P. This is followed by the selection of h(.), Ǥ and Dz. Here, Ǥ takes β as input and returns $\bar{Q}_i \in \{0,1\}^{Ľ}$. On the other hand, Dz takes in

$β^*$ and $ꞵ_i$. Here, the hamming distance H_D between the previously entered user biometrics β and the latter entered biometrics $β^*$ should be less than ȳ. In essence, the output is a function of the initial biometric key $Ǭ_i$= Dz($β^*$, $ꞵ_i$). Finally, the AMF keeps PK_A privately but publishes the parameter set {E_p(f,g), p, P, h(.), PUK_A, Ǥ(.),Dz(.), ȳ}.

Step 2: For each gNB, the AMF chooses unique identity ID_{gNB} and private key $Ħ_{PR}$. It then derives the equivalent public key $Ħ_{PU}$= $Ħ_{PR}$.P. Next, it publishes $Ħ_{PU}$, computes security token $Ū_{gNB}$=h(ID_{gNB}||$Ħ_{PR}$) and buffers {ID_{gNB}, $Ū_{gNB}$, $Ħ_{PU}$}. Thereafter, it composes message $ϻ_1$={ID_{gNB}, $Ħ_{PR}$, $Ū_{gNB}$} before sending it to the gNB through some secure channels.

Step 3: The UE selects unique identity ID_{UE}, private key $Ψ_{PR}$ and then computes its equivalent public key $Ψ_{PU}$= $Ψ_{PR}$.P. Next, the UE derives $Ū_{UE}$ = h(ID_{UE}||$Ψ_{PR}$) and then transmits Reg_{Req} together with $Ū_{gNB}$ to the AMF through some secure channels.

Step 4: Upon receipt of this message, the AMF computes A_i=h($Ū_{UE}$||PK_A) before sending it to the UE through some secure channels.

Step 5: On receiving A_i, the UE selects some secret token Ꝁ before prompting the user to imprint β at its sensor. It then derives the following parameters:

Ǥ(β)= ($Ǭ_i$, $ꞵ_i$)
B_i=h(Ꝁ||$Ψ_{PR}$||ID_{UE}||$Ǭ_i$)
A_i^*= $A_i \oplus$h(ID_{UE}||Ꝁ||$Ǭ_i$)
$Ψ_{PR}^*$= $Ψ_{PR} \oplus$h(ID_{UE}||$Ǭ_i$)

The UE stores {$Ψ_{PR}^*$, B_i, Ǥ(.), Dz(.), $ꞵ_i$, h(.), ȳ} before publishing $Ψ_{PU}$ and substituting A_i with A_i^* in its memory.

3.2 Authentication and Key Agreement Phase

During this phase, the UE and gNB are mutually authenticated before establishing the session key that they use to encipher the exchanged packets. It is executed in six major phases as discussed below.

Step 1: The user inputs ID_{UE}^*, $Ꝁ^*$ before imprinting $β^*$ at the UE's sensor. Next, the UE derives $Ǭ_i^*$= Dz($β^*$, $ꞵ_i$), $Ψ_{PR}^{**}$= $Ψ_{PR}^* \oplus$h($ID_{UE}^* \oplus Ǭ_i^*$) and B_i^*=h($Ꝁ^*$||ID_{UE}^*||$Ψ_{PR}^*$||$Ǭ_i^*$). It then checks whether B_i^*=B_i holds and if not, the session is aborted. However, if it holds, the UE selects random nonce R∈ Z_p^* , generates current timestamp $τ_1$ before computing the following security parameters: C_i= R.P=(($C_i)_χ$, $(C_i)_y$), D_i= R.PUK_A=($(D_i)_χ$, $(D_i)_y$), $Ū_{UE}^*$ = h($Ψ_{PR}^*$||ID_{UE}^*), E_{UE}=$Ū_{UE}^* \oplus (D_i)_y$, E_{gNB}=ID_{gNB} $^* \oplus (D_i)_y$, A_i^{**}= $A_i^* \oplus$h(ID_{UE}^*||$Ꝁ^*$||$Ǭ_i^*$), F_i=h(ID_{gNB}||$τ_1$||D_i||A_i^{**}), G_i=$(D_i)_χ$, H_i=(F_i+$G_i Ψ_{PR}^{**}$)R^{-1} mod p. Finally, the UE composes message $ϻ_2$={E_{UE}, E_{gNB}, C_i, $τ_1$, G_i, H_i} before forwarding it to the AMF over some public channels.

Step 2: After receiving $ϻ_2$ from the UE, the AMF determine current timestamp $τ_2$ followed by the confirmation of whether $τ_2$-$τ_1 \leq Δτ$ such that if this condition does not hold, the authentication is dropped. However, if this verification is successful, the AMF computes K= PK_A.C_i=($(K)_χ$, $(K)_y$), $Ū_{UE}^*$=$E_{UE} \oplus (K)_y$), ID_{gNB}^*=$E_{UE} \oplus (K)_y$), A_i=h($Ū_{UE}^*$||PK_A) and F_i^*=h(ID_{gNB}^*||$τ_1$||K||A_i). Next, the AMF checks whether ID_{gNB}^* is in its database and if it is not, authentication process is dropped. However, if it is, the AMF computes S_1=H_i^{-1} mod p, S_2=$F_i^* S_1$ mod p, S_3= G_i S_1 mod p, D_i^*=($(D_i)_χ$, $(D_i)_y$)=(S_2.P+ S_3.$Ψ_{PU}$)PK_A. Here:

$$(S_2.P+S_3.Ψ_{PU})PK_A=(((F_i^*.P/H_i)+(((G_iΨ_{PR}).P/H_i))PK_A=(H_i^{-1})(F_i^*+G_iΨ_{PR})PK_A.P$$
$$=(H_i^{-1})(RH_i)PK_A.P=R(PUK_A)=D_i=((D_i)_χ, (D_i)_y).$$

This is followed by the confirmation of whether G_i= $(D_i^*)_χ$=$(D_i)_χ$= G_i. If this condition does not hold, the session is dropped, otherwise the UE is successfully authenticated by the AMF.

Step 3: The AMF then selects random nonce ¥∈ Z_p^*, followed by the determination of its current timestamp τ_3. Next, it computes $ƛ=¥.P=((ƛ)_\chi, (ƛ)_y$, $Ǟ=h(A_i||\tau_1)\oplus h(C_i||Ū_{gNB}||\tau_3||\tau_1)$, $ȓ=(ƛ)_\chi$, $ɭ=¥^{-1}(h(A_i||\tau_1)+ ȓPK_A)$ mod p. Afterwards, the AMF constructs message $ɱ_3=\{Ǟ, \tau_3, \tau_1, C_i, ƛ, ɭ\}$ and sends it to the gNB over insecure channels.

Step 4: Upon receipt of $ɱ_3$, the gNB determines its current timestamp τ_4, and checks if τ_4-$\tau_3 \le \Delta\tau$. If this condition does not hold, authentication process is dropped, otherwise the gNB derives $h(A_i||\tau_1)= Ǟ)\oplus h(C_i||Ū_{gNB}||\tau_3||\tau_1)$, $ɤ= ɭ^{-1}$ mod p, $ɦ= h(A_i||\tau_1)_ɤ$ mod p, $ȓ=(ƛ)_\chi$, $ɸ=ȓɤ$ mod p, $ƛ^*=ɦ.P+ɸ.PUK_A=((ƛ^*)_\chi, (ƛ^*)_y$. Here, $ɦ.P+ɸ.PUK_A=h(A_i||\tau_1)_{ɤ.P}+ȓɤ(PK_A.P)= ɤ(h(A_i||\tau_1)+ȓPK_A.P=(ɭ^{-1})(¥ɭ).P=¥.P=ƛ=((ƛ^*)_\chi, (ƛ^*)_y$. This is followed by the confirmation of whether $ȓ^*=(ƛ^*)_\chi=(ƛ)_\chi= ȓ$, and if this condition is false, authentication is dropped. However, if this condition is true, AMF is validated by the gNB.

Step 5: The gNB selects random nonce Б∈ Z_p^*, determines its current timestamp τ_5 before checking whether τ_5-$\tau_4 \le \Delta\tau$. If this condition does not hold, authentication process is dropped, otherwise it derives $Ʊ=Б.C_i= Б(R.P)$, $ᶃ=h(ID_{gNB}||h(A_i||\tau_1||Ʊ||\tau_1||\tau_5)$, $Ⱬ= Б.P=((Ⱬ)_\chi, (Ⱬ)_y$, $ɠ=(Ⱬ)_\chi$ and $ȡ=Б^{-1}(h(ᶃ)+ɠĦ_{PR})$ mod p. Afterwards, the gNB composes response message $ɱ_4=\{Ⱬ, ȡ, \tau_5\}$ before transmitting it to the UE via public channels.

Step 6: Upon receiving $ɱ_4$ at timestamp τ_6, the UE determines whether τ_6-$\tau_5 \le \Delta\tau$ and if this is false, authentication session is dropped. However, if this verification is successful, the UE has successfully validated the gNB and hence proceeds to re-compute the session key. This begins by having the UE derive $Ʊ^*=R.Ⱬ=R.(Б.P)=Ʊ$, $ᶃ^*=h(ID_{gNB}||h(A_i^*||\tau_1||Ʊ^*||\tau_1||\tau_5)$, $ʝ=ȡ^{-1}$ mod p, $ʧ=h(ᶃ*)ʝ$ mod p, $ƶ=ɠʝ$ mod p, $Ⱬ^*= ʧ.P+ƶĦ_{PU} =((Ⱬ^*)_\chi, (Ⱬ^*)_y$. Here, $ʧ.P+ƶĦ_{PU} =(h(ᶃ^*)_ʝ).P+(ɠʝĦ_{PR}).P=ʝ(h(ᶃ^*)+ɠĦ_{PR}).P= ȡ^{-1}(Б.ȡ).P= Б.P=((Ⱬ)_\chi, (Ⱬ)_y$. This is followed by the confirmation of whether $ɠ^*=(Ⱬ^*)_\chi =(Ⱬ)_\chi=ɠ$ and if this condition is false, authentication is dropped, otherwise the UE sets the session key as $ᶃ^*= ᶃ$ to secure its communication with the gNB.

4 SECURITY ANALYSIS

In this section, it is proved that the user through the UE establishes a session key with the gNB before the onset of packet exchanges. In addition, it is proved that the UE authenticates the user before permission is accorded to initiate the communication process. To accomplish this, Burrows–Abadi–Needham (BAN) logic is deployed. The process involves the verification of the sources of all the exchanged messages, freshness checks of the exchanged beacons and also the establishment of trust among the communicating entities. The BAN logic notations and postulates in [25] and [26] are deployed for these proofs. The two goals to be proved are formulated as follows:

Goal-1: $UE|\equiv (UE \overset{g}{\leftrightarrow} gNB)$

Goal-2: $gNB|\equiv (UE \overset{g}{\leftrightarrow} gNB)$

The initial state assumptions (ISAs) in this protocol are formulated as follows:

ISA$_1$: $UE|\equiv\#(\tau_1)$, $UE|\equiv\#(\tau_5)$

ISA$_2$: $AMF|\equiv\#(\tau_1)$, $UE|\equiv\#(\tau_3)$

ISA$_3$: $gNB|\equiv\#(\tau_1)$, $gNB|\equiv\#(\tau_3)$, $gNB|\equiv\#(\tau_5)$

ISA$_4$: $AMF|\equiv\ AMF \overset{R.P}{\longleftrightarrow} gNB$

ISA$_5$: $gNB|\equiv\ AMF \overset{R.P}{\longleftrightarrow} gNB$

ISA$_6$: $gNB|\equiv AMF \Rightarrow |\sim S$

ISA$_7$: $UE|\equiv (UE \overset{Б.P}{\longleftrightarrow} gNB)$

ISA$_8$: $gNB|\equiv (UE \overset{Б.P}{\longleftrightarrow} gNB)$

ISA$_9$: $UE|\equiv gNB \Rightarrow (UE \overset{g}{\leftrightarrow} gNB)$

The BAN logic based proofs (BLPs) then proceed through the formulation of various lemmas as follows:

During the authentication and key agreement phase, messages $\text{Ӎ}_2=\{E_{UE}, E_{gNB}, C_i, \tau_1, G_i, H_i\}$, $\text{Ӎ}_3=\{\text{Ǟ}, \tau_3, \tau_1, C_i, \text{ƛ}, \text{ɭ}\}$ and $\text{Ӎ}_4=\{\text{Ȥ}, \text{ʠ}, \tau_5\}$ are exchanged among the communicating entities. The generic form of these messages can be expresses as follows:

Msg-1: $\text{AMF}\rightarrow\text{gNB}\{(h(A_i\|\tau_1)\ )\oplus h(R.P\|\bar{U}_{gNB}\|\tau_3\|\tau_1), \text{¥}.P, \text{¥}^{-1}(h(A_i\|\tau_1)+PK_A(\text{¥}.P)_\chi, R.P, \tau_3, \tau_1\}$
Msg-2: $\text{gNB}\rightarrow\text{UE}\{\text{Б}.P, \text{Б}^{-1}(h(h(ID_{gNB}\|h(A_i\|\tau_1)\|\text{Б}.R.P\|\tau_1\|\tau_5))+ \text{ʠ}\Psi_{PR}(\text{Б}.P)_\chi), \tau_5)$

In an idealized form, messages Ӎ_2 and Ӎ_3 can be written as follows:

Msg-1: $\langle < ((A_i||\tau_1), \left(R.P\,\middle|\middle|\bar{U}_{gNB}\middle|\middle|\,\tau_1\middle||\tau_3)\right), \text{¥}.P, \left((A_i||\tau_1), PK_A(\text{¥}.P)\right), \tau_3, \tau_1 >\rangle_{\text{AMF}\overset{R.P}{\longleftrightarrow}\text{gNB}}$

Msg-2: $\langle < \left(\text{UE}\overset{g}{\leftrightarrow}\text{gNB}\right), \text{ʠ}\Psi_{PR}(\text{Б}.P)_\chi)), \tau_5 >\rangle_{\text{UE}\overset{\text{Б}.P}{\longleftrightarrow}\text{gNB}}$

Based on Msg-1, BLP$_1$ is obtained:

BLP$_1$: $\text{gNB}\lhd\langle < ((A_i||\tau_1), \left(R.P\,\middle|\middle|\bar{U}_{gNB}\middle|\middle|\,\tau_1\middle||\tau_3)\right), \text{¥}.P, \left((A_i\middle|\middle|\tau_1), PK_A(\text{¥}.P)\right), \tau_3, \tau_1 >\rangle_{\text{AMF}\overset{R.P}{\longleftrightarrow}\text{gNB}}$

Applying MMR to BLP$_1$ and ISA$_5$ results in BLP$_2$:

BLP$_2$: $\text{gNB}|\equiv\text{AMF}|\sim\langle < ((A_i||\tau_1), \left(R.P\,\middle|\middle|\bar{U}_{gNB}\middle|\middle|\,\tau_1\middle||\tau_3)\right), \text{¥}.P, \left((A_i\middle|\middle|\tau_1), PK_A(\text{¥}.P)\right), \tau_3, \tau_1 >\rangle$

Next, both NVR and FR are applied in BLP$_2$ and ISA$_3$ to yield BLP$_3$:

BLP$_3$: $\text{gNB}|\equiv\text{AMF}|\equiv\langle < ((A_i||\tau_1), \left(R.P\,\middle|\middle|\bar{U}_{gNB}\middle|\middle|\,\tau_1\middle||\tau_3)\right), \text{¥}.P, \left((A_i\middle|\middle|\tau_1), PK_A(\text{¥}.P)\right), \tau_3, \tau_1 >\rangle$

The application of BR and JR in BLP$_3$ and ISA$_6$ results in BLP$_4$:

BLP$_4$: $\text{gNB}|\equiv\ (A_i||\tau_1)$

On the other hand, using BR on BLP$_4$, BLP$_5$ is obtained:

BLP$_5$: $\text{gNB}|\equiv(\text{UE}\overset{g}{\leftrightarrow}\text{gNB})$, hence **Goal-2** is achieved.

According to Msg-2, BLP$_6$ is obtained:

BLP$_6$: $\text{UE}\lhd\langle < \left(\text{UE}\overset{g}{\leftrightarrow}\text{gNB}\right), \text{ʠ}\Psi_{PR}(\text{Б}.P)_\chi)), \tau_5 >\rangle_{\text{UE}\overset{\text{Б}.P}{\longleftrightarrow}\text{gNB}}$

Afterwards, MMR is used in both BLP$_6$ and ISA$_7$ to yield BLP$_7$:

BLP$_7$: $\text{UE}|\equiv\text{gNB}|\sim\langle < \left((\text{UE}\overset{g}{\leftrightarrow}\text{gNB}\right), \text{ʠ}\Psi_{PR}(\text{Б}.P)_\chi)), \tau_5 >\rangle$

On the other hand, the application of BR, FR and NVR in BLP$_7$ and ISA$_1$ results in BLP$_8$:

BLP$_8$: $\text{UE}|\equiv\text{gNB}|\equiv\ \text{UE}\overset{g}{\leftrightarrow}\text{gNB}$

According to BLP$_8$ and ISA$_9$, JR is applied to obtain BLP$_9$:

BLP$_9$: $\text{UE}|\equiv(\text{UE}\overset{g}{\leftrightarrow}\text{gNB})$, thus **Goal-1** is attained.

As such, the attainment of both Goal-1 and Goal-2 proofs that the UE and gNB mutually authenticate each other with the help of the AMF as an intermediary.

5 CONCLUSION

The criticality of security and privacy issues during the communication over 5G HetNets has seen the 3GPP specify three AKA protocols. However, many attacks have been designed against these three protocols, rendering them ineffective. Consequently, other authentication schemes have been developed. However, past research has shown that these protocols are still vulnerable to other attacks, while some of them are inefficient for resource limited 5G HetNets devices. The developed protocol has been demonstrated to validate all message sources, carry out freshness checks and setup a session key for traffic protection. This potentially thwarts packet replays, session hijacking, privacy leakages and impersonation attacks. Future work lies in performance evaluation of the proposed protocol as well as its informal analysis.

REFERENCES

[1] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, “5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view,” IEEE Access, 6, 55765–55779, 2018.

[2] 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), IEEE, 11-15, 2021.

[3] 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.

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

[5] M. Hojjati, A. Shafieinejad, and H. Yanikomeroglu, “A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks,” IEEE Access, 8, 216461-216476, 2020.

[6] [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.

[7] H. Bagheri, M. Noor-A-Rahim, Z. Liu, H. Lee, D. Pesch, K. Moessner, and P. Xiao, “5G NR-V2X: Toward Connected and Cooperative Autonomous Driving,” IEEE Communications Standards Magazine, 5(1), 48-54, 2021.

[8] M. Chen, C. Tan, X. Zhu, and X. Zhang, “A Blockchain-Based Authentication and Service Provision Scheme for Intemet of Things,” in 2020 IEEE Globecom Workshops (GC Wkshps), 1-6, IEEE, 2020.

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

[10] 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.

[11] 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.

[12] R. Borgaonkar, H. Lucca, P. Shinjo, and S. Altaf, “New privacy threat on 3G, 4G, and upcoming 5G AKA protocols,” in Proc. Privacy Enhancing Technol., 3, 108-127, 2019.

[13] J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A. C.K. Soong, and J.C. Zhang, “What will 5G be?” J. Sel. Areas Commun., 32(6),1065–1082, 2014.

[14] 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.

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

[16] V.O. Nyangaresi and S.O. Ogundoyin, “Certificate Based Authentication Scheme for Smart Homes**,”** in 2021 3rd Global Power, Energy and Communication Conference (GPECOM)**,** IEEE**,** 202-207, 2021.

[17] C. Qiu, F.R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, “Blockchain based software-defined industrial Internet of Things: A dueling deep Q-learning approach,” IEEE Internet of Things Journal, 6(3), 4627-4639, 2018.

[18] T. Anithaashri, G. Ravichandran, and R. Baskaran, “Security enhancement for software defined network using game theoretical approach,” Computer Networks, 157, 112-121, 2019.

[19] N.Z. Bawany and J. A. Shamsi, “SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks,” Journal of Network and Computer Applications, 145, 102381, 2019.

[20] 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.

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

[22] M. Ouaissa, A. Rhattoy, and M. Lahmer, “Group access authentication of machine to machine communications in LTE networks,” The second international conference on Internet of Things, data and cloud computing (ICC 2017), 1-5, 2017.

[23] 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.

[24] C.I. Fan, Y.T. Shih, J.J. Huang, and W.R. Chiu, “Cross-network-slice authentication scheme for the 5 th generation mobile communication system,” IEEE Transactions on Network and Service Management, 18(1), 701-712, 2021.

[25] V.O. Nyangaresi and M.A. Morsy, “Towards Privacy Preservation in Internet of Drones,” in 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), IEEE, 306-311, 2021.

[26] V.O. Nyangaresi, “Lightweight Key Agreement and Authentication Protocol for Smart Homes,” in 2021 IEEE AFRICON, 1-6. IEEE, 2021.