Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.032044
Article

Tech Science Press

An Enhanced Group Key-Based Security Protocol to Protect 5G SON Against FBS

Hoonyong Park[1], TaeGuen Kim[1], Daniel Gerbi Duguma[1], Jiyoon Kim[2], Ilsun You[2,*] and Willy Susilo[3]

[1]Department of Information Security Engineering, Soonchunhyang University, Asan-si, 31538, Korea
[2]Department of Financial Information Security, Kookmin University, Seoul-si, 02707, Korea
[3]Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, 2522, Australia
*Corresponding Author: Ilsun You. Email: ilsunu@gmail.com
Received: 04 May 2022; Accepted: 30 June 2022

Abstract: Network operators are attempting many innovations and changes in 5G using self-organizing networks (SON). The SON operates on the measurement reports (MR), which are obtained from user equipment (UE) and secured against malware and userspace programs. However, the synchronization signal block that the UE relies on to measure the wireless environment configured by a base station is not authenticated. As a result, the UE will likely gauge the wrong wireless environment configured by a false base station (FBS) and transmit the corresponding MR to the serving base station, which poisons the data used for 5G SONs. Therefore, the serving base stations must verify the authenticity of the MR. The 3GPP has advocated numerous solutions for this issue, including the use of public key certificates, identity-based keys, and group keys. Although the solution leveraging group keys have better efficiency and practicality than the other two, they are vulnerable to security threats caused by key leaks via insiders or malicious UE. In this paper, we analyze these security issues and propose an improved group key protocol that uses a new network function, called a broadcast message authentication network function (BMANF), which validates broadcasted messages on behalf of the UE. The protocol operates in two phases: initial and verification. During the initial phase, the 5G core network distributes a shared secret key to the BMANF and UE, allowing the latter to request an authentication ticket from the former. During the verification phase, the UE requests the BMANF to validate the broadcasted messages received from base stations using the ticket and its corresponding shared key. For evaluation, we formally verified the proposed protocol, which was then compared with alternative methods in terms of computing cost. As a result, the proposed protocol fulfills the security requirements and shows a lower overhead than the alternatives.

Keywords: False base station; NR measurement report; 5G network; self-organizing network

1 Introduction

The introduction of enhanced mobile broadband and superior reliability (and low latency) with coverage for a high density of devices in the fifth-generation mobile networks has transformed several sectors and unlocked new services. The self-organizing network (SON) plays an important role in such networks by improving the overall network performance through self-x functions such as automatic configuration, healing, and optimization [1]. The primary goal of the SON is to supply intelligence to mobile networks to facilitate network organization, setup, optimization, and recovery. Furthermore, it minimizes total network complexities, capital expenditure, and operating expenses [2–5]. SONs anticipate that future networks will be paired with sophisticated algorithms to ensure higher network performance than that of previous generations of mobile networks. Such critical improvements combined with autonomous learning will enable future mobile networks to be much more proactive and adaptable than present mobile networks.

SON applications primarily target access network components, with important applications such as load balancing, mobility management, handover optimization, and backhaul optimization [6]. As a result, SON features operate at a high level by collecting and analyzing the measurement reports (MR) from user equipment (UE) connected to the network. However, there is a security risk of data poisoning, also known as SON poisoning, in which an attacker infiltrates the MR using a malicious UE or a false base station (FBS) [7]. This security issue can cause cell outages and signaling floods, as well as denial-of-service (DoS) attacks on both the UE and network [8]. UE is typically unable to verify the veracity of System Information (SI) messages transmitted from gNodeB or 5G base station (gNB) and may use them to communicate MR (possibly containing bogus information) to the gNB to which they are currently connected. Such unauthenticated messages would then lead to SON poisoning attacks.

To defend against such attacks, two major techniques, i.e., cryptographic and intrusion detection and prevention, can be considered. Our discussion is based on the previous line of defense, which was offered by 3GPP in three categories: public key certificate (PKC)-, identity-based cryptography (IBC)-, and group key-based schemes [7]. The first two schemes use asymmetric keys to protect over-the-air intruders that replay previously recorded SI messages or send malevolently constructed ones aiming to poison the SONs. Although these approaches play a significant role in authenticating broadcast message (BM) without presharing secret keys, they possess a high computational overhead because of their expensive operations. Additionally, while the primary solution requires costly public key infrastructure (PKI) to manage digital signatures and public key encryption, the IBC lacks practicality and has a key escrow problem [9]. In contrast, the group key-based scheme depends on the collaboration of the serving network (SN) and home network (HN) for the dynamic supply of session keys and computation of message authentication codes between the UE and gNB. Nevertheless, the solution has security concerns regarding insider threats. An attacker with a genuine UE can gain access to a shared group key from the different groups to which it belongs. We explain these security mechanisms in depth in Section 2.

Inspired by the previous technique presented, we analyze the security problem and propose an improved version of it. In each group, the enhanced protocol uses a new network function to verify the BM on behalf of the UE. The following are the main contributions of this paper:

- By analyzing and improving the security concerns of the group key-based solution, we design a secure and authentication ticket-based protocol that prohibits the UE from sharing a group key. Moreover, through the Burrows–Abadi–Needham (BAN) logic [10] and Automated Validation of Internet Security Protocols and Applications (AVISPA) [11], we formally verify the protocol and show that it satisfies the security requirements of mutual authentication and secure key exchange.
- In terms of performance and security, we compare the proposed protocol to group key-, PKC-, and IBC-based solutions. As a result, we demonstrate that the proposed scheme achieves a better performance than the alternative solutions.

The rest of the paper is structured as follows: Section 2 discusses the 5G SON security threats and their proposed countermeasures. Section 3 describes our proposed protocol, and Section 4 presents its formal verification. Section 5 outlines a comparative analysis of the proposed protocol compared with other proposed solutions. Finally, Section 6 concludes the paper.

2 Security Threats and Existing Countermeasures of SON in 5G

This section discusses two security vulnerabilities in the context of 5G: authentication relay attack and SON data contamination. Furthermore, we describe the key cryptographic schemes to counter these attacks (e.g., PKC-, IBC-, and group key-based methods).

2.1 Security Threats

Wireless attackers can send maliciously crafted MR through the UE using their software-defined radio (SDR) or build a wireless environment to generate distorted MR around genuine UE through FBS, as illustrated in Fig. 1a. In more detail on the latter, the FBS may collect cell IDs of adjacent regular base stations and use one of them to impersonate a real base station. Subsequently, it can create a radio environment disguised as a genuine base station to trick UE into generating an MR based on that environment and transmitting it to the serving base station. This attack is possible because the UE cannot verify the received SI and thus cannot determine whether the adjacent base station is false.

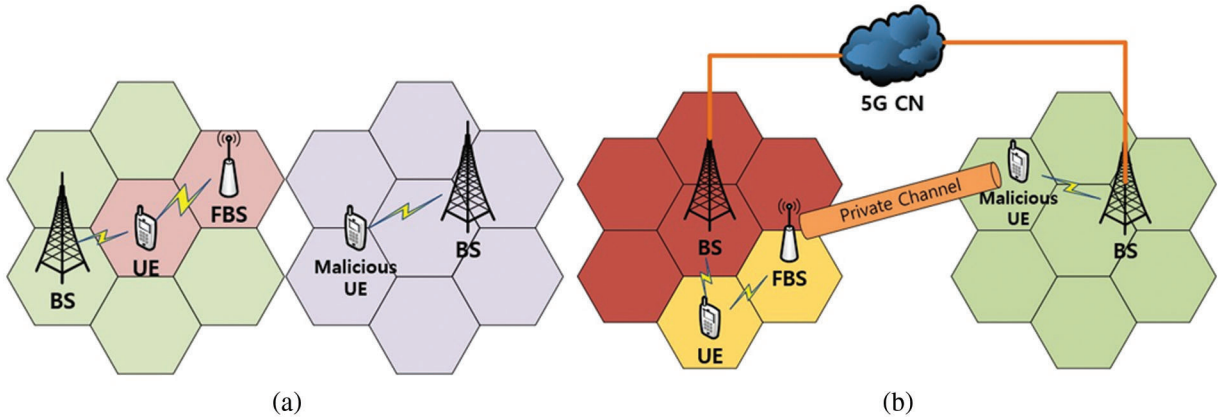

Figure 1: An illustration of (a) SON contamination and (b) Authentication relay attacks

However, there is a more complex scenario in which the FBS and malicious UE are far apart and connected by local or wide area networks to form vicious links. First, the FBS induces access to the victim UE and transmits an initial registration request message to the malicious UE. The malicious UE then transmits the received message to the core network through a remote legitimate base station. Then, in reverse order, the FBS and malicious UE forward the response message sent by the core network to the UE to complete the authentication. By relaying the base station physically separated in this way, an attacker may cause the UE to report the signal strength of the FBS to the legitimate base station, inducing confusion in the network SON configuration. Fig. 1b shows the authentication relay attack.

2.2 Existing Countermeasures

Few studies (such as [12,13]) proposed various mechanisms to counteract the FBS. However, in this paper, we focus on those proposed by 3GPP: PKC-, IBC-, and group key-based schemes [7].

2.2.1 Public Key Certificate-based Solutions

PKC-based countermeasures enable the UE to validate the authenticity of the BM that gNBs disseminate without the need for sharing the signing key. During the "Registration Accept" and "Location Update Accept" messages exchanged between AMF and UE, the former sends the latter a list of tracking area IDs along with the corresponding public keys and lifespan. The network operator also provides the matching private keys to the NR, which it will use to sign the SI with other information like time counter, downlink frequency, and physical cell ID. The inclusion of this extra information hinders replay attacks. The NR then broadcasts the digital signature along with the least significant bits of time counter (to address errors introduced because of time counter differences between the UE and access network) and the SI. The UE verifies the digital signature and time counter using the stored public key for that particular tracking area. Public key-based solutions can also use the PKI to protect the SI. The gNB signs the BM with its private key and sends it to the UE along with a plain message and its certificate. The UE then verifies the received certificate with the root certificate provided at the manufacturing time or during the "Registration Accept" message. In both of these solutions, digitally signing SI can be delegated to a new network function called digital signing network function (DSnF).

2.2.2 Identity-based Cryptographic-based Solutions

IBC-based countermeasure is another method for SI verification. In this technique, the core network provides different credentials to the NR and UE for the certificateless signature algorithm. It also provides the NR with a private signing key for signing SI and a public validation token unique to each cell for validating the signature to the UE. An additional solution in this category leverages the private key generator (PKC) along with the public and private keys. The public key is programmed into the UE, either at manufacturing time or through the non-access stratum security mode command complete message, whereas the private key is kept secret. Subsequently, the PKC use the identity of the gNB and its private key to derive a signing key for the gNB. Once the BM with a digital signature is received, the UE verifies it using PKC's public key and gNB's identity (which can be reconstructed from the BM).

2.2.3 Group Key-based Solution

The group key-based method for protecting the BM operates among the UE, SN, and HN of the 5G environment. The SN automatically supplies the UE (specifically mobile equipment (ME)) with keys of the gNBs, which are ciphered with the assistance of the HN and cannot be deciphered by the ME. As shown in Fig. 2, the solution consists of three phases: protection key agreement and transfer (PKAT), protection area (PA) information provisioning (PAIP), and cell authentication procedure. In the first phase, the protection key CK_p is agreed upon between the HN (AUSF/UDM) and UE, and the same key is transferred to the SN (AMF/SEAF) for the subsequent procedures. It is worth noting that because the long-term key is found only in the universal subscriber identity module (USIM) and HN, only the USIM can correctly compute CK_p. During the PAIP procedure, the SN provides the encrypted root keys of groups (called share root key group (SRKG)) in the PA to the UE, which optimizes the number of encrypted keys supplied to the ME. The SRKG is represented by a group key identifier (GKI), whereas the gNBs in an SRKG are identified by a unique group node identifier (GNI). The SN provides the GKI and GNI to the corresponding gNB and computes K_{BS} = HMAC-SHA-256 (K_{RBS}, <GKI, GNI>), where K_{RBS} is a root key shared by a group of gNBs. The SN then provides K_{BS} to the corresponding gNB. Once these initial setups have been completed, the SN obtains the list of PA information (including GKI, EK_{RBS}, and lifetime, where EK_{RBS} is K_{RBS} encrypted with CK_p) based on the UE's request for registration. It then returns the registration response with the PA information back to the UE. In the final phase, the gNB computes the message authentication code (MAC_i) of the SI (including GKI and GNI) and downlink frequency with K_{BS}. It then broadcasts the GKI and GNI with the MAC_i, where the UE receives and checks whether the GKI exists in the PA information. If so, the ME sends the EK_{RBS}, <GKI,

GNI> to the USIM, in which the latter decrypts the EK_{RBS} (using CK_p) to K_{RBS}, computes the K_{BS} based on K_{RBS}, and computes the expected message authentication code ($xMAC_i$). Subsequently, the USIM sends the $xMAC_i$ to the ME to compare it with the MAC_i.

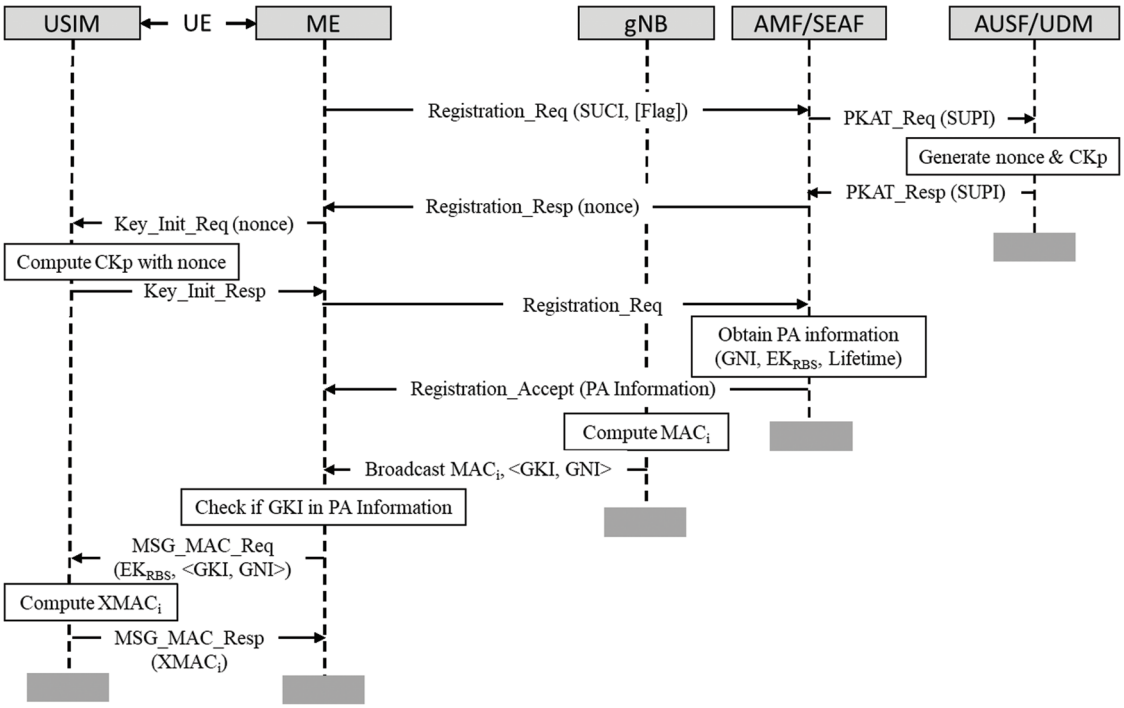

Figure 2: Group key-based solution to counteract the FBS

3 Proposed Protocol

The proposed protocol is an improved version of the group key-based solution proposed in [7]. Although the original group key-based technique has some advantages, including enhanced computing efficiency and lessened group administration costs, it has a substantial security flaw, primarily because the root key K_{RBS} (technically the EK_{RBS}) is shared with the UE. As a result, if an attacker compromises one group member or joins multiple groups with a legitimate UE (but with malicious intent), the group key can be revealed, allowing legitimate gNBs to be masqueraded. Hence, we propose a network function called a BM authentication network function (BMANF) to tackle this problem and validate the BM instead of the UE. In addition to this, we addressed other security concerns with the solution. Tab. 1 outlines the descriptions of the notations used in this protocol.

3.1 System Model

The main difference between the proposed protocol and the 3GPP candidate solution is validating the BM. In the latter case, the UE performs the verification process, whereas the former uses a BMANF in each group to verify the BM. Fig. 3 shows the system model of the proposed protocol.

Before transmitting the MR to the serving gNB, the UE contacts the BMANF to verify the received BM using its HMAC. The BMANF uses its own K_{RBS} to derive the K_{BS} of each base station, confirms the HMAC, and informs the UE about the result. As a result, even if the FBS delivers a BM, the BMANF may validate it before the UE transmits the MR to the gNB, preventing the gNB from receiving an erroneous MR. Hence, handover attempts to the FBS are blocked, and the quality of data for the SON functions is preserved.

Table 1: Notations used in the proposed protocol

Notations	Descriptions
K_X	The secret key of an entity X
K_{X-Y}	The shared key between entities X and Y
ID_X	Unique identifier of an entity X
$Ticket_X$	Ticket for entity X
K_{Ticket}	Key to redeem the ticket
$Expire_T$	Expiry time of a ticket
K_{RBS}	Root key of a share root key group
K_{BS}	Key to each base station
$Timestamp_n$	n^{th} timestamp
$E(K, M)$	Symmetric encryption of a message M using a key K
$HMAC(K, M)$	Hash-based message authentication code of a message M using a key K
$List[A, B]$	List of A and B tuples
$\|$	Concatenation symbol

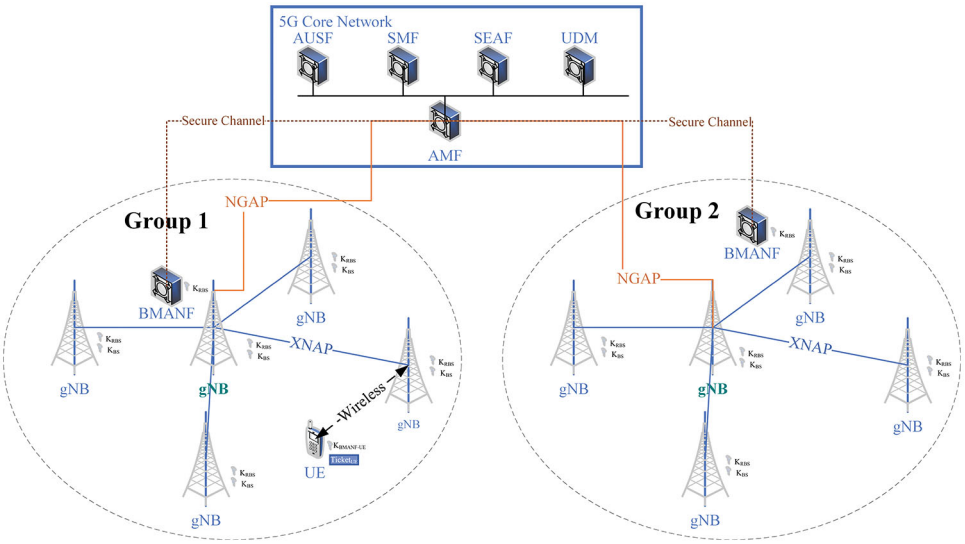

Figure 3: System model for the proposed protocol

3.2 Threat Model

To securely exchange messages over insecure channels, protocols must be safe from passive attackers who compromise confidentiality by eavesdropping on messages and active attackers who violate the integrity and availability of communications by modifying and deleting messages. The attackers can also be malicious insiders or unauthorized outsiders. The Dolev–Yao (DY) model [14] is best suited to modeling the threats emanating from such security problems. A DY attacker is a powerful adversary that can eavesdrop on all messages transmitted, including those between the UE and gNB, and knows all the proposed protocol procedures. Furthermore, it can exchange messages with communication participants and forge,

retransmit, or even delete messages. However, this attacker cannot decrypt a ciphered message without the correct encryption key, recover the result of a one-way hash function, and guess random numbers.

3.3 Security Requirements

The primary goal of the proposed protocol is to protect the BM authentication procedure in the 5G environment. Therefore, it must meet essential security requirements like a secure key exchange and mutual authentication. Secure key exchange prescribes a safe key establishment procedure that will be used to encrypt and guard communications, whereas mutual authentication refers to the property that entities establish each other's identity before real communication begins.

3.4 Assumptions

Several gNBs within the tracking area managed by one AMF constitute different groups. The root key, K_{RBS}, is shared by all the gNBs in each group. The K_{RBS} is provisioned to the gNB and updated periodically by the AMF. Each gNB derives the K_{BS} from the K_{RBS} using their group identifier and calculating the HMAC of the message when transmitting a BM. The formula to derive the K_{BS} is shown in Eq. (1).

$$K_{BS} = HMAC(K_{RBS}, \ \langle ID_{Group}, \ ID_{gNB} \rangle) \tag{1}$$

The UE and AMF know the algorithm to derive the shared key between the BMANF and UE, $K_{BMANF\text{-}UE}$, from K_{AMF}. The BMANF communicates with the AMF by establishing a secure channel. Furthermore, it is assumed that all nodes are time synchronized.

3.5 The Initial Phase

Fig. 4 shows the procedure of the initial phase of the proposed protocol. In this phase, the $K_{BMANF\text{-}UE}$ is distributed using the existing 5G registration mechanism. Following the AS security activation, the UE requests a ticket from the BMANF, which it uses for authentication in subsequent sessions. The following are the specifics of the initial phase.

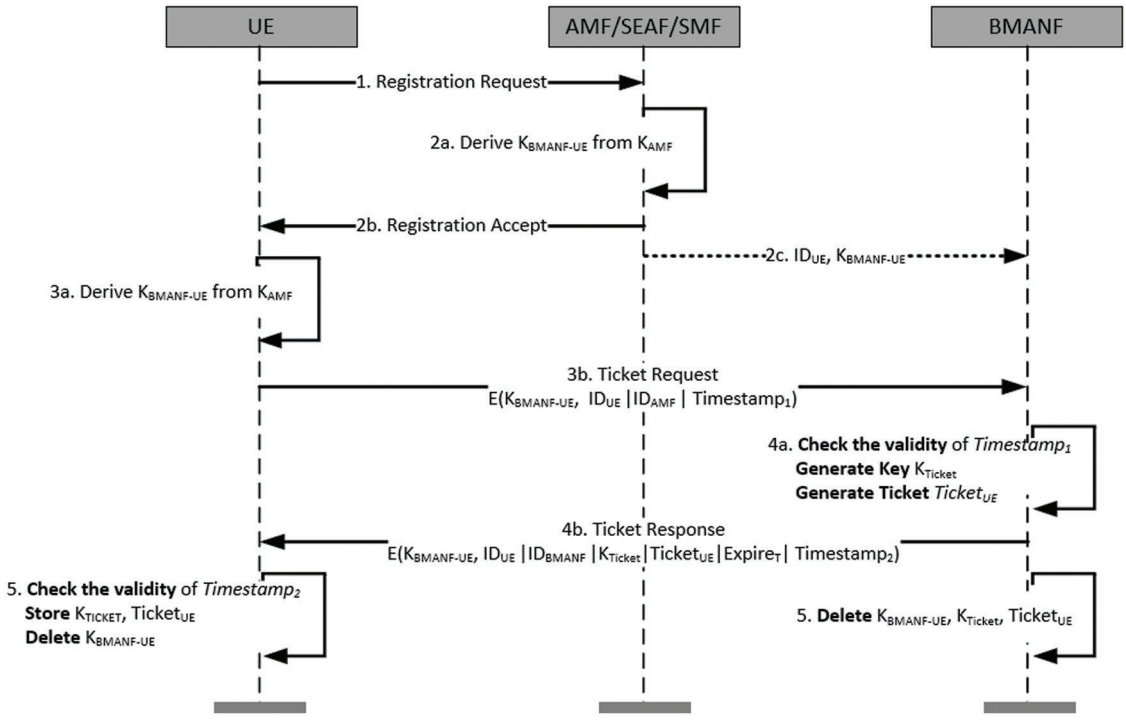

Figure 4: Initial phase of the proposed protocol

Step 1: This step follows the registration request procedure defined in 3GPP TS 38.331 [15], TS 38.413 [16], and TS 33.501 [17].

Steps 2a–2c: The AMF derives the $K_{BMANF\text{-}UE}$ from the K_{AMF} and transmits message 2b to the UE following the registration accept procedure defined in the standard, such as in Step 1, and then delivers the $K_{BMANF\text{-}UE}$ to the BMANF.

Steps 3a and 3b: The UE derives the $K_{BMANF\text{-}UE}$ from the K_{AMF} in the same way that the AMF did. Then, using the $K_{BMANF\text{-}UE}$, it encrypts the Temporary Mobile Subscriber Identity (*TMSI*) by including ID_{UE}, ID_{AMF}, and $Timestamp_1$. It should be noted that ID_{UE} is a UE's pseudo identity, a structure comparable to the 5G globally unique temporary identification (5G-GUTI). The actual computation of ID_{UE} is outside the scope of this study. Finally, the UE requests a ticket by sending the ticket request message that includes the ID_{UE} and encrypted *TMSI* to the BMANF.

Steps 4a and 4b: The BMANF decrypts the message with the $K_{BMANF\text{-}UE}$, verifies $Timestamp_1$, and if valid, creates K_{Ticket} and $Ticket_{UE}$. The $Ticket_{UE}$ is constructed as shown in Eq. (2).

$$Ticket_{UE} = E(K_{BMANF},\ \ ID_{UE}|ID_{AMF}|ID_{BMANF}|K_{Ticket}|Expire_T) \tag{2}$$

Next, the BMANF prepares a "Ticket Response" message by encrypting the ID_{UE}, ID_{BMANF}, K_{Ticket}, $Ticket_{UE}$, $Expire_T$, and $Timestamp_2$ with the $K_{BMANF\text{-}UE}$ and transmits it to the UE.

Step 5: The UE verifies the validity of $Timestamp_2$, and if the verification succeeds, it stores the K_{Ticket} and $Ticket_{UE}$. Following that, the UE and BMANF delete $K_{BMANF\text{-}UE}$ from their memory to assure perfect forward secrecy.

3.6 The Verification Phase

The verification phase begins once the initial phase is completed. When the UE triggers the MR transmission condition set via MeasConfig, before transmitting the MR to the serving gNB, the UE dispatches the BM of the adjacent gNBs used to create the MR and its HMAC to the BMANF for a verification request. According to the verification result, the UE transmits an MR to the serving gNB or creates a new one. When the UE requests verification from the BMANF, it transmits the $Ticket_{UE}$ together for authentication. Fig. 5 shows the procedure of the verification phase, and its description is presented as follows:

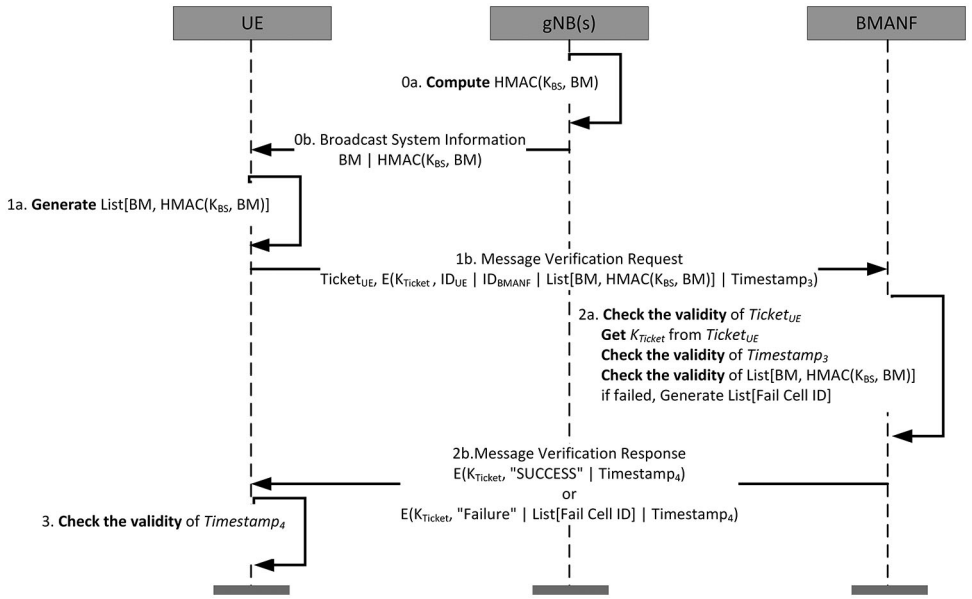

Figure 5: Verification phase of the proposed protocol

Steps 0a and 0b: The gNBs use their K_{BS} to generate the HMAC of the BM. The gNBs transmit the BM with the corresponding HMAC values to nearby UE.

Steps 1a and 1b: The UE creates a list of BMs and HMAC values received from different gNBs that will be used to generate the MR. To request the BMANF for BM verification, the UE encrypts the BM, its HMAC list, and $Timestamp_3$ with K_{Ticket} and transmits the $Ticket_{UE}$ together.

Steps 2a and 2b: The BMANF decrypts the $Ticket_{UE}$ using its secret key, K_{BMANF}, and then reads the K_{Ticket}. Next, it verifies $Timestamp_3$ and, if valid, confirms the HMAC of the BMs. If confirmation succeeds, the BMANF transmits a success message with $Timestamp_4$. If not, the BMANF creates a list of filed BMs and sends it along with a message of failure.

Step 3: The UE verifies$Timestamp_4$ after receiving the message verification response message. If valid, it transmits an MR to the serving base station. If not, the UE generates an MR, except for the gNB that failed verification, and transmits it to the serving gNB.

Tab. 2 summarizes the approaches, pros, and cons of the solutions proposed by 3GPP and our proposed protocol.

Table 2: Summary of the approaches, benefits, and drawbacks of several FBS defense mechanisms

Schemes	Technique	Merits	Limitations
PKC	UE relies on PKI to authenticate the signed BM and certificate received using the gNBs' and Certificate Authority's public keys. The DSnF can also be used to compute the digital signature of the BM on behalf of the cells.	• No need for preshared security keys • More practical and widely used • Better efficiency when the signature is delegated to DSnF	• Expensive to manage the PKI keys and certificates • Higher computational overhead due to public key operations
IBC	The UE counts on the PKG (which generates the private keys for gNBs and set their identities as public keys) to verify the signed BM received from gNBs using PKG's public key and gNB's identity.	• More lightweight than PKC-based solutions from the UE side • Less expensive than the PKC scheme as there is no need for certificate management	• Lacks practicality and has a key escrow problem • Needs a private interface between the gNB and PKG
Group key	The UE depends on the group keys shared among clusters of base stations to verify the BM received from the gNBs using a symmetric key algorithm (i.e., message authentication code).	• Cheaper than both the PKC and IBC as it uses symmetric key-based authentication codes • Enhanced computational efficiency and lessened group administration costs	• Vulnerable to malicious UE, i.e., an insider threat that allows legitimate gNBs to be masqueraded
Proposed protocol	The approach improves the group key technique such that UE and BMANF share a secret key and the latter provides the former with an authentication ticket. The UE, hence, banks on the BMANF (using the ticket and its corresponding shared key) to validate the BM received from the gNBs.	• Defend against malicious UE-initiated insider threats • With the help of the BMANF, the malicious BM can be filtered, relieving the gNBs • Can serve as a framework for more advanced applications such as blockchain and machine learning	• Exhibits a higher communication overhead (due to the placement of the BMANF) traded for improved security

4 Formal Security Verification

This section analyzes the security of the proposed protocol using two well-known verification tools: BAN logic and AVISPA.

4.1 BAN Logic-Based Formal Verification

BAN logic, named after its three creators, Burrows, Abadi, and Needham, uses distinct notations and rules to verify security protocols based primarily on belief deductions. BAN logic's verification procedure consists of four steps: idealization (modeling the protocol using formal logic), assumption (setting initial realistic security assumptions), goals (defining the security objectives that the protocol is expected to meet), and derivation (deriving the security goals from the rules, assumptions, and intermediate results of the derivation). The BAN logic notations and rules can be found in [18] and [19]. The reader is also referred to Appendices B and C for the notations and rules, respectively. The following is the formal verification of the proposed protocol using the BAN logic.

4.1.1 Initial Phase

Idealization. Here, all messages that are not protected (for instance through encryption) are excluded. The idealized initial phase of the proposed protocol is shown as follows.

$$UE \rightarrow BMANF: \ \langle ID_{UE}, \ ID_{BMANF}, \ TS_1, \ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF \rangle_{K_{BMANF-UE}} \tag{II1}$$

$$BMANF \rightarrow UE: \ \langle ID_{UE}, \ ID_{BMANF}, \ TS_2, \ UE \overset{K_T}{\longleftrightarrow} BMANF, \ TICKET_{UE}, \ EXP_{TICKET}, \ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF \rangle_{K_{BMANF-UE}} \tag{II2}$$

Assumption. The assumptions that the BMANF and UE make regarding security keys and the freshness of the timestamps are shown in (IA1) and (IA2), and (IA3)–(IA5), respectively.

$$BMANF \ | \equiv BMANF \overset{K_{BMANF-UE}}{\longleftrightarrow} UE \tag{IA1}$$

$$BMANF \ | \equiv \#(TS_1) \tag{IA2}$$

$$UE \ | \equiv BMANF \overset{K_{BMANF-UE}}{\longleftrightarrow} UE \tag{IA3}$$

$$UE \ | \equiv \#(TS_2) \tag{IA4}$$

$$UE \ | \equiv BMANF \ | \Rightarrow \ UE \overset{K_T}{\longleftrightarrow} BMANF \tag{IA5}$$

Goal. The security goals of the initial phase of the protocol regarding the secure exchange of identities and the preshared secret key ($K_{BMANF\text{-}UE}$) are formulated in (IG1)–(IG4), respectively. (IG5) denotes a successful ticket key allocation from the BMANF to the UE.

$$BMANF \ | \equiv UE \ | \equiv ID_{UE} \tag{IG1}$$

$$BMANF \ | \equiv \ UE \ | \equiv \ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF \tag{IG2}$$

$$UE \ | \equiv BMANF \ | \equiv ID_{BMANF} \tag{IG3}$$

$$UE \ | \equiv \ BMANF \ | \equiv \ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF \tag{IG4}$$

$$UE \ | \equiv UE \overset{K_T}{\longleftrightarrow} BMANF \tag{IG5}$$

Derivation. As shown in (ID1)–(ID12), the security goals are derived by applying the idealization, assumptions, and BAN logic rules.

From (II1):

$$BMANF \triangleleft ID_{UE},\ \langle ID_{AMF},\ TS_1,\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF\rangle_{K_{BMANF-UE}} \tag{ID1}$$

$$BMANF\ |\equiv\ UE\ |\sim\ [ID_{UE},\ ID_{AMF},\ TS_1,\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF]\ by\ (D1),\ (A1),\ MM \tag{ID2}$$

$$BMANF\ |\equiv\ UE\ |\equiv\ [ID_{UE},\ ID_{AMF},\ TS_1,\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF]\ by\ (D2),\ (A2),\ FR,\ NV \tag{ID3}$$

$$BMANF\ |\equiv\ UE\ |\equiv\ ID_{UE}\ by\ (D3),\ BC \tag{ID4}$$

$$BMANF\ |\equiv\ UE\ |\equiv\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF\ by\ (D3),\ BC \tag{ID5}$$

From (II2):

$$UE \triangleleft ID_{UE},\ \langle ID_{BMANF},\ TS_2,\ UE \overset{K_T}{\longleftrightarrow} BMANF,\ TICKET_{UE},\ EXP_{TICKET},\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF\rangle_{K_{BMANF-UE}} \tag{ID6}$$

$$UE\ |\equiv\ BMANF\ |\sim [ID_{UE},\ ID_{BMANF},\ TS_2,\ UE \overset{K_T}{\longleftrightarrow} BMANF,\ TICKET_{UE},\ EXP_{TICKET},\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF]by\ (D6),\ (A3),\ MM \tag{ID7}$$

$$UE\ |\equiv\ BMANF\ |\sim [ID_{UE},\ ID_{BMANF},\ TS_2,\ UE \overset{K_T}{\longleftrightarrow} BMANF,\ TICKET_{UE},\ EXP_{TICKET},\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF]by\ (D7),\ (A4),\ FR,\ NV \tag{ID8}$$

$$UE\ |\equiv\ BMANF\ |\equiv\ ID_{BMANF}\ by\ (D8),\ BC \tag{ID9}$$

$$UE\ |\equiv\ BMANF\ |\equiv\ UE \overset{K_{BMANF-UE}}{\longleftrightarrow} BMANF\ by\ (D8),\ BC \tag{ID10}$$

$$UE\ |\equiv\ BMANF\ |\equiv\ UE \overset{K_T}{\longleftrightarrow} BMANF\ by\ (D8),\ BC \tag{ID11}$$

$$UE\ |\equiv\ UE \overset{K_T}{\longleftrightarrow} BMANF\ by\ (D11),\ (A5),\ JR \tag{ID12}$$

From the aforementioned derivations (ID1)–(ID12), it is possible to see that all goals have been derived. The following theorem and lemmas illustrate this fact.

Theorem 1: The initial phase of the proposed protocol is secure.

Proof: From Lemma 1–1 and Lemma 1–2, the defined goals are satisfied, and hence, the initial phase of the proposed protocol is secure.

Lemma 1–1: The initial phase of the proposed protocol supports mutual authentication.

Proof: The derived belief (ID4) shows that the BMANF authenticates the UE, and (ID9) shows that the UE authenticates the BMANF. From this, the initial phase of the proposed protocol can provide mutual authentication.

Lemma 1–2: The initial phase of the proposed protocol provides secure key exchange.

Proof: The BMANF trusts the $K_{BMANF\text{-}UE}$ assigned by the AMF as defined in (IA1). Furthermore, the UE believes that the $K_{BMANF\text{-}UE}$ can be derived from K_{AMF} as defined in (IA3). Hence, (ID5) and (ID10) show that both UE and BMANF can believe $K_{BMANF\text{-}UE}$ indirectly.

4.1.2 Verification Phase

Idealization. The idealization for the verification phase is given as follows.

$$BMANF \rightarrow BMANF:\ \langle ID_{UE},\ ID_{AMF},\ ID_{BMANF},\ UE \overset{K_T}{\longleftrightarrow} BMANF,\ EXP_{TICKETK}\rangle_{BMANF} \tag{AI1}$$

$$UE \rightarrow BMANF:\ ID_{UE},\ \langle ID_{BMANF},\ TS_1,\ UE \overset{K_T}{\longleftrightarrow} BMANF\rangle_{K_T},\ \langle BM,\ BMANF \overset{K_{BS}}{\longleftrightarrow} gNB\rangle_{K_{BS}} \tag{AI2}$$

$$BMANF \rightarrow UE:\ ID_{UE},\ \langle ID_{BMANF},\ TS_2,\ ACK,\ UE \overset{K_T}{\longleftrightarrow} BMANF\rangle_{K_T} \tag{AI3}$$

Assumption. The first five assumptions are for the BMANF, whereas the remaining two assumptions are for the UE concerning symmetric keys and the freshness of the ticket and timestamp.

$$BMANF\ |\equiv BMANF \overset{K_{BMANF}}{\longleftrightarrow} BMANF \tag{AA1}$$

$$BMANF\ |\equiv \#(EXP_{TICKET}) \tag{AA2}$$

$$BMANF\ |\equiv\ BMANF\ |\Rightarrow\ UE \overset{K_T}{\longleftrightarrow} BMANF \tag{AA3}$$

$$BMANF\ |\equiv \#(TS_1) \tag{AA4}$$

$$BMANF\ |\equiv BMANF \overset{K_{BS}}{\longleftrightarrow} gNB \tag{AA5}$$

$$UE\ |\equiv BMANF \overset{K_T}{\longleftrightarrow} UE \tag{AA6}$$

$$UE\ |\equiv \#(TS_2) \tag{AA7}$$

Goal. Goals (AG1)–(AG4) are for the BMANF, whereas (AG5) and (AG7) are for the UE.

$$BMANF\ |\equiv\ UE \overset{K_T}{\longleftrightarrow} BMANF \tag{AG1}$$

$$BMANF\ |\equiv UE\ |\equiv ID_{UE} \tag{AG2}$$

$$BMANF\ |\equiv\ UE\ |\equiv\ UE \overset{K_T}{\longleftrightarrow} BMANF \tag{AG3}$$

$$BMANF\ |\equiv\ UE\ |\sim\ BM \tag{AG4}$$

$$UE\ |\equiv\ BMANF\ |\equiv ID_{BMANF} \tag{AG5}$$

$$UE\ |\equiv\ BMANF\ |\equiv ACK \tag{AG6}$$

$$UE\ |\equiv\ BMANF\ |\equiv\ UE \overset{K_T}{\longleftrightarrow} BMANF \tag{AG7}$$

Derivation. The aforementioned goals (AG1)–(AG7) are derived as follows.

From (AI1):

$$BMANF \triangleleft ID_{UE},\ ID_{AMF},\ \langle ID_{BMANF},\ UE \overset{K_T}{\longleftrightarrow} BMANF,\ EXP_{TICKETK}\rangle_{BMANF} \tag{AD1}$$

$$BMANF\ |\equiv\ BMANF\ |\sim\ [ID_{UE},\ ID_{AMF},\ ID_{BMANF},\ UE \overset{K_T}{\longleftrightarrow} BMANF,\ EXP_{TICKET}]\ by\ (D1),\ (A1),\ MM \tag{AD2}$$

$$BMANF \mid\equiv BMANF \mid\equiv [ID_{UE}, ID_{AMF}, ID_{BMANF}, UE \overset{K_T}{\longleftrightarrow} BMANF, EXP_{TICKET}] \; by \; (D2), (A2), FR, NV \quad \text{(AD3)}$$

$$BMANF \mid\equiv BMANF \mid\equiv UE \overset{K_T}{\longleftrightarrow} BMANF \; by \; (D3), BC \quad \text{(AD4)}$$

$$BMANF \mid\equiv UE \overset{K_T}{\longleftrightarrow} BMANF \; by \; (D4), (A3), JR \quad \text{(AD5)}$$

From (AI2):

$$BMANF \triangleleft ID_{UE}, \langle ID_{BMANF}, TS_1, UE \overset{K_T}{\longleftrightarrow} BMANF\rangle_{K_T}, \langle BM, BMANF \overset{K_{BS}}{\longleftrightarrow} gNB\rangle_{K_{BS}} \quad \text{(AD6)}$$

$$BMANF \mid\equiv UE \mid\sim [ID_{UE}, ID_{BMANF}, TS_1, UE \overset{K_T}{\longleftrightarrow} BMANF] \; by \; (D6), (D5), MM, BC \quad \text{(AD7)}$$

$$BMANF \mid\equiv UE \mid\equiv [ID_{UE}, ID_{BMANF}, TS_1, UE \overset{K_T}{\longleftrightarrow} BMANF] \; by \; (D7), (A4), FR, NV \quad \text{(AD8)}$$

$$BMANF \mid\equiv UE \mid\equiv ID_{UE} \; by \; (D8), BC \quad \text{(AD9)}$$

$$BMANF \mid\equiv UE \mid\equiv UE \overset{K_T}{\longleftrightarrow} BMANF \; by \; (D8), BC \quad \text{(AD10)}$$

$$BMANF \mid\equiv UE \mid\sim [BM, BMANF \overset{K_{BS}}{\longleftrightarrow} gNB] \; by \; (D6), (A5), MM, BC \quad \text{(AD11)}$$

$$BMANF \mid\equiv UE \mid\sim BM \; by \; (D11), BC \quad \text{(AD12)}$$

From (AI3):

$$UE \triangleleft ID_{UE}, ID_{BMANF}, TS_2, ACK, UE \overset{K_T}{\longleftrightarrow} BMANF_{K_T} \quad \text{(AD13)}$$

$$UE \mid\equiv BMANF \mid\sim [ID_{UE}, ID_{BMANF}, TS_2, ACK, UE \overset{K_T}{\longleftrightarrow} BMANF] \; by \; (D13), (A6), MM \quad \text{(AD14)}$$

$$UE \mid\equiv BMANF \mid\equiv [ID_{UE}, ID_{BMANF}, TS_2, ACK, UE \overset{K_T}{\longleftrightarrow} BMANF] \; by \; (D14), (A7), FR, NV \quad \text{(AD15)}$$

$$UE \mid\equiv BMANF \mid\equiv ID_{BMANF} \; by \; (D15), BC \quad \text{(AD16)}$$

$$UE \mid\equiv BMANF \mid\equiv ACK \; by \; (D15), BC \quad \text{(AD17)}$$

$$UE \mid\equiv BMANF \mid\equiv UE \overset{K_T}{\longleftrightarrow} BMANF \; by \; (D15), BC \quad \text{(AD18)}$$

According to the aforementioned derivation (AD1)–(AD18), all goals (AG1)–(AG7) are achieved. The following theorem and lemmas illustrate these goals.

Theorem 2: The verification phase of the proposed protocol is secure.

Proof: From Lemma 2–1 to Lemma 2–3, the defined goals are satisfied, and hence, the verification phase of the proposed protocol is secure.

Lemma 2–1: The verification phase of the proposed protocol provisions mutual authentication.

Proof: The derived belief (AD9) shows that the BMANF authenticates the UE, and (AD16) shows that the UE authenticates the BMANF. From this, it is possible to show that the protocol provides mutual authentication.

Lemma 2–2: The secret key K_{Ticket} is successfully exchanged between the UE and BMANF.

Proof: The UE and BMANF have a direct belief in the secret key K_{Ticket} through (AA6) and (AD5). Conversely, the indirect belief of the UE and BMANF in the secret key K_{Ticket} can be proved with (AD10) and (AD18).

Lemma 2–3: The verification phase of the proposed protocol provides confidentiality and integrity.

Proof: From the aforementioned Lemma 2–2, the secret key K_{Ticket} is successfully communicated between the UE and BMANF. Hence, the verification phase of the proposed protocol provides confidentiality and integrity with K_{Ticket}.

In conclusion, both initialization and verification phases of the proposed protocol are proven to be secure through Theorems 1 and 2.

4.2 AVISPA-based Simulation

The BAN logic has limitations when it comes to accurately specifying a protocol, particularly during the idealization step [20]. Accordingly, automated formal verification tools alongside BAN logic are often used to complement the limitations. In this section, we use AVISPA to verify the proposed protocol formally. AVISPA uses a unique language called the high-level specification language (HLPSL) to describe the protocol and security property. The HLPSL specification is translated into the intermediate format (IF) through the HLPSL2IF. The translated IF specification is entered into each verification module of the AVISPA to analyze the defined security goals.

The HLPSL specification consists of three roles: basic, session, and environment. The basic role defines protocol participants' specifications and initial information and expresses message exchange between protocol participants. Session role defines parameters and channels for protocol session participants. The environment role declares the protocol and overall specification of sessions and attackers. The basic roles of each agent are depicted in Figs. 6 and 7, and the AVISPA verification result for the proposed protocol using the on-the-fly model checker and constraint-logic-based attack searcher is shown in Fig. 8. The results confirm that the proposed protocol is secure for the set of security properties.

```
role ue(U, G, B: agent, KBU: symmetric_key,
SND_G, RCV_G, SND_B, RCV_B: channel(dy)
)played_by U def=

local
      State: nat,
      Reg_req, Reg_ac, TS1, TS2, BM, TS3, TS4: text,
      KT: symmetric_key,
      TICKET, BM_MAC: message

init
      State := 0

transition
1.    State = 0     ∧ RCV_G(start) =|>
      State' := 2   ∧ Reg_req' := new() ∧ SND_G(Reg_req')
2.    State =2      ∧ RCV_G(Reg_ac') =|>
      State' := 5   ∧ TS1' := new() ∧ SND_B({U.G.TS1'}_KBU)
                      ∧ secret(KBU,key_bmanf_ue,{U,B})
3.    State = 5     ∧ RCV_B({U.B.KT'.TICKET'.TS2'}_KBU) =|>
      State' := 7
4.    State = 7     ∧ RCV_G(BM'.BM_MAC') =|>
      State' := 9   ∧ TS3' := new()
                    ∧ SND_B(TICKET.{U.G.BM'.BM_MAC'.TS3'}_KT)
5.    State = 9     ∧ RCV_B({TS4'}_KT) =|>
      State' := 11
end role
```

(a)

```
role bmanf(U,G,B: agent, KB, KG, KGB: symmetric_key,
HM: hash_func, SND_U, RCV_U, SND_G, RCV_G: channel(dy)
)played_by B def=

local
      State: nat,
      TS1, TS2, BM, TS3, TS4: text,
      TICKET: message,
      KBU, KT: symmetric_key

init
      State := 2

transition
1.    State = 2     ∧ RCV_G({U.KBU'}_KGB) =|>
      State' := 4

2.    State = 4     ∧ RCV_U({U.G.TS1'}_KBU) =|>
      State' := 6   ∧ TS2' := new() ∧ KT' := new()
                    ∧ TICKET' := {U.B.KT'}_KB
                    ∧ SND_U({U.B.KT'.TICKET'.TS2'}_KBU)

3.  State = 6
    ∧ RCV_U({U.B.KT}_KB.{U.G.BM'.HM(KG.BM').TS3'}_KT) =|>
    State' := 10  ∧ TS4' := new() ∧ SND_U({TS4'}_KT)
end role
```

(b)

Figure 6: Basic roles for (a) UE and (b) BMANF

```
role gnb(U,G,B: agent, KBU,KGB, KG: symmetric_key,
HM: hash_func, SND_U, RCV_U, SND_B, RCV_B: channel(dy)
)played_by G def=

local
        State: nat,
        Reg_req, Reg_ac, BM: text,
        BM_MAC: message

init
        State := 1

transition
1.      State = 1       /\ RCV_U(Reg_req') =|>
        State' := 3     /\ Reg_ac' := new() /\ BM' := new()
                        /\ BM_MAC' := HM(KG.BM')
                        /\ SND_U(Reg_ac')
                        /\ SND_B({U.KBU}_KGB)
                        /\ SND_U(BM'.BM_MAC')
end role
```

Figure 7: Basic roles for gNB

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/hoon2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s
  visitedNodes: 52 nodes
  depth: 10 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/hoon2.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 14 states
  Reachable  : 8 states
  Translation: 0.01 seconds
  Computation: 0.00 seconds
```

Figure 8: AVISPA verification result for the proposed protocol

5 Comparative Analysis

This section presents the performance and security comparison results of the proposed protocol against the PKC-, IBC-, group key-based, and DSnF schemes [12]. Tab. 3 shows the latency of the cryptographic operations, and Tab. 4 compares the performance and security of these solutions against our protocol. We measure the computational overhead using the Apple MacBook Pro M1 max 64 GB RAM.

Table 3: Delay time by cryptographic operation

Computation	Latency (ms)
Symmetric encryption/decryption (C_1)	1.000
ECDSA (C_2)	11.000
ECDSA validation (C_3)	33.000
One-way HMAC (C_4)	10.002
ID-based digital signature algorithm (C_5)	20.233
ID-based digital signature algorithm validation (C_6)	31.000
Round-trip time (UE ↔ BMANF) (RTT)	414

Table 4: Performance and security comparison of FBS defense schemes

Schemes	Performance			Security			
	UE	gNB (s)	Delegation (BMANF/DSnF)	SA	MI	AV	IT
PKC based	$k * 2C_3$	$k * C_2$		●	●	◑	●
IBC based	$k * C_6$	$k * C_5$		●	●	◑	○
Group key based	$k * C_4$	$k * C_4$		●	●	○	○
DSnF	$k * 2C_3$	$C_1 + C_4$	$k * C_2 + C_1 + C_4$	●	●	◑	●
Proposed protocol (Total)	$4 * C_1 + 1$ RTT	$k * C_4$	$2 * C_1 + k * C_4$	●	●	●	●

Note: n, number of gNBs neighboring the UE; **SA**, sender authentication; **MI**, message integrity; f, frequency of broadcasting SI; **AV**, availability; **IT**, defense against insider threat.
$k = n * f$; ○: low ◑: medium ●: high

On the basis of the results of Tabs. 3 and 4, Fig. 9 depicts a series of graphs that illustrate the computational overhead against the density of the gNBs (with *f* ranging from low to medium to high), broadcast per second (with *n* ranging from low to medium to high), and round-trip time (with both *f* and *n* ranging from low to medium to high). The greater the number of adjacent base stations and the shorter the broadcast period, the more cryptographic operations must be performed. Furthermore, the higher the roundtrip time, the higher the latency of the proposed protocol. To compare the overhead of each method with the environment, an experiment was conducted. It is worth noting that the overhead in the graph is the total computational cost of the UE, gNBs, and network functions (BMANF and DSnF).

According to Fig. 9, the performance of the PKC, IBC, and DSnF schemes persistently shows significantly higher overhead as the density of the gNBs and their broadcast frequency increase. Such high loads are exhibited mainly because of the costly certificate transport and heavy Elliptic Curve Digital Signature Algorithm for the PKC and Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption for the IBC. Compared with the group key-based solutions (the original and enhanced), the disparity in computational cost widens as the density and broadcast frequency increases, which makes the PKC, IBC, and DSnF solutions less desirable.

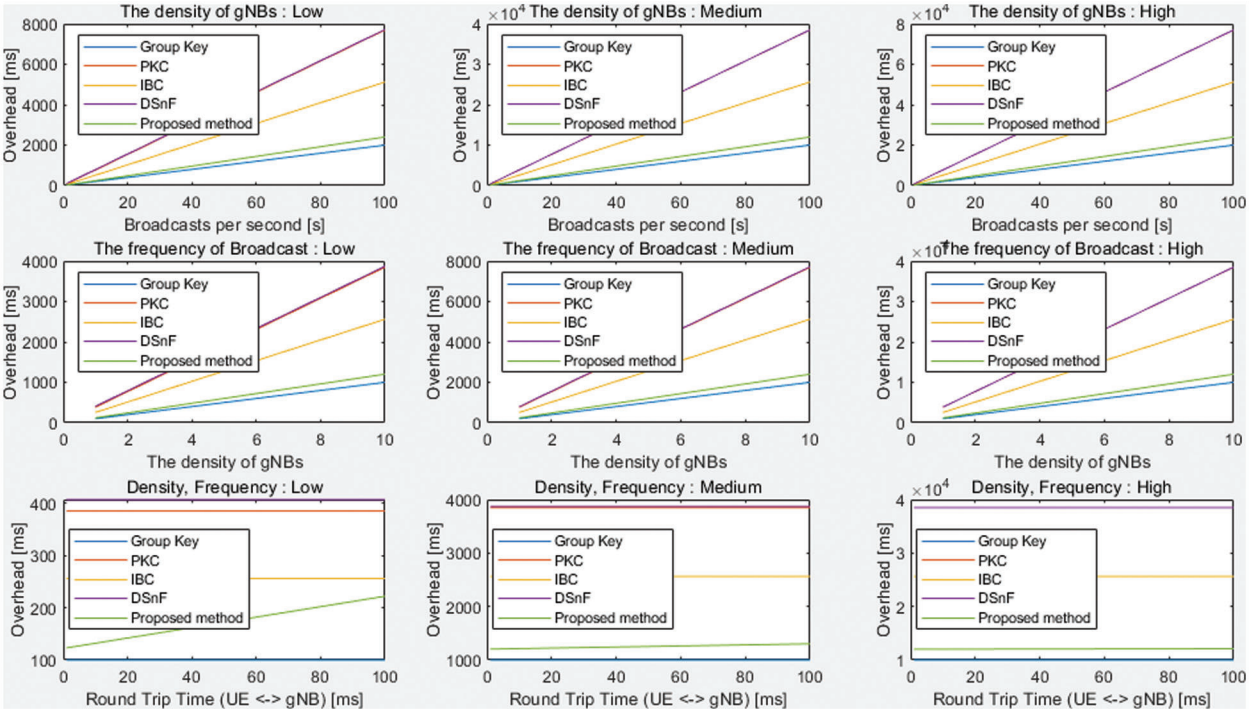

Figure 9: Performance comparison of different FBS defense mechanisms

Concerning the group key-based schemes, the original group key-based solution shows a slightly lower overhead as the density of the gNBs and broadcast frequency grow. In terms of the round-trip time, the proposed solution exhibits a higher overhead (compared with the group key-based solution) due to the addition of the BMANF, which is located near the gNB control unit). However, the burden of the UE (which is computationally resource constrained) in the proposed solution is less. In contrast, the UE in the other solutions perform frequent computations as the BM transmission period is short. Furthermore, the proposed protocol addresses critical security flaws found in the group key-based scheme while also satisfying all the four security requirements itemized in Tab. 4. Therefore, the proposed protocol is secure, efficient, and suitable, especially in environments where the computing resource of the UE is limited.

6 Conclusions

This paper proposes a security protocol that can prevent the FBS and improve the quality of data for the SON functions, thereby safeguarding networks from SON-poisoning attacks. The suggested protocol is divided into two phases: initial and verification. During the first phase, the AMF distributes a shared key $K_{BMANF\text{-}UE}$ to the UE and BMANF. Following that, the UE securely requests an authentication ticket from the BMANF using the shared key. The UE then requests that the BMANF validate the BM received from the gNBs using the authentication token obtained during the verification phase. The UE determines whether or not to transmit the MR to the base station based on the verification result. The proposed protocol has also been formally verified using the BAN logic and AVISPA. The verification findings reveal that initial and verification phases of the protocol are secure and satisfy the specified security requirements. Furthermore, in terms of computational cost, we compared our protocol with the PKC-, IBC-, and group key-based protocols given in 3GPP TR 33.809. As a result, particularly in resource-limited contexts, our technique has been demonstrated to be more efficient and beneficial than competing solutions detailed in Section 2.2. However, the proposed approach has some limitations that cannot be

avoided when a hostile UE using SDR sends a counterfeit MR to the serving gNB. Other security solutions, such as an intrusion detection system, are required for such special cases because it is difficult to respond to an FBS using only cryptographic techniques. As follow-up research, we would like to use the BMANF to investigate machine learning-based techniques (such as designing anomaly detection algorithms) for detecting the MR emitted by hostile UE.

Funding Statement: This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability, 100%)

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] O. G. Aliu, A. Imran, M. A. Imran and B. Evans, "A survey of self-organization in future cellular networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 336–361, 2013.

[2] P. V. Klaine, M. A. Imran, O. Onireti and R. D. Souza, "A survey of machine learning techniques applied to self-organizing cellular networks," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2392–2431, 2017.

[3] P. V. Klaine, O. Onireti, R. D. Souza and M. A. Imran, "The role and applications of machine learning in future self-organizing cellular networks," in *Next-Generation Wireless Networks Meet Advanced Machine Learning Applications*, Hershey, Pennsylvania, USA: IGI Global, pp. 1–23, 2019. https://www.igi-global.com/about/.

[4] M. D. Cia, F. Mason, D. Peron, F. Chiariotti, M. Polese *et al.,* "Using Smart City Data in 5G Self-Organizing Networks," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 645–654, 2018.

[5] A. Imran, A. Zoha and A. Abu-Dayya, "Challenges in 5G: How to empower SON with big data for enabling 5G," *IEEE Network*, vol. 28, no. 6, pp. 27–33, 2014.

[6] H. Fourati, R. Maaloul, L. Chaari and M. Jmaiel, "Comprehensive survey on self-organizing cellular network approaches applied to 5G networks," *Computer Networks*, vol. 199, pp. 108435, 2021.

[7] SA3, "3rd generation partnership project; technical specification group services and system aspects study on 5G security enhancement against false base stations (FBS) (Release 17)," 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539.

[8] A. Shaik, R. Borgaonkar, S. Park and J. P. Seifert, "On the impact of rogue base stations in 4G/LTE self organizing networks," in *Proc. WiSec*, New York, NY, USA, pp. 75–86, 2018.

[9] K. Emura, S. Katsumata and Y. Watanabe, "Identity-based encryption with security against the KGC: A formal model and its instantiations," *Theoretical Computer Science*, vol. 900, pp. 97–119, 2022.

[10] M. Burrows, M. Abadi and R. M. Needham, "A logic of authentication," *Proceeding of the Royal Society of London: A Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[11] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna *et al.,* "AVISPA tool for the automated validation of internet security protocols and applications," in *Proc. CAV*, Edinburgh, Scotland, UK, pp. 281–285, 2005.

[12] H. Gao, Y. Zhang, T. Wan, J. Zhang and H. Duan, "On evaluating delegated digital signing of broadcasting messages in 5G," in *Proc. GLOBECOM*, Waikoloa, HI, USA, pp. 1–7, 2019.

[13] P. K. Nakarmi, M. A. Ersoy, E. U. Soykan and K. Norrman, "Murat: Multi-RAT false base station detector," *arXiv e-prints*, vol. 2102, no. 8780, pp. 1–13, 2021.

[14] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transaction on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[15] RAN2, "3rd generation partnership project; technical specification group radio access network; NR; radio resource control (RRC) protocol specification (Release 16)," 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3197.

[16] RAN3, "3rd generation partnership project; technical specification group radio access network; NG-RAN; NG application protocol (NGAP) (Release 16)," 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3223.

[17] SA3, "3rd generation partnership project; technical specification group services and system aspects; security architecture and procedures for 5G system (Release 17)," 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

[18] J. Kim, D. G. Duguma, P. V. Astilo, H. Y. Park, B. Kim *et al.,* "A formally verified security scheme for inter-gNB-DU handover in 5G vehicle-to-everything," *IEEE Access*, vol. 9, pp. 119100–119117, 2021.

[19] D. G. Duguma, J. Kim, S. Lee, N. S. Jho, V. Sharma *et al.,* "A lightweight D2D security protocol with request-forecasting for next-generation mobile networks," *Connection Science*, vol. 34, no. 1, pp. 362–386, 2021.

[20] C. Boyd and W. Mao, "On a limitation of BAN logic," in *Proc. EUROCRYPT*, Lofthus, Norway, pp. 240–247, 1993.

Appendix A Abbreviations

Abbreviation	Full name
AMF	Access and Mobility Function
AS	Access stratum
AUSF	Authentication
BM	Broadcast Message
BMANF	Broadcast Message Authentication Network Function
CAP	Cell Authentication Procedure
DSnF	Digital Signing Network Function
ECCSI	Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption
ECDSA	Elliptic Curve Digital Signature Algorithm
FBS	Fake Base Station
GKI	Group Key Identifier
gNB	g-NodeB (5G Base Station)
gNB-CU	gNB Control Unit
GNI	Group Node Identifier
HMAC	Hash-based message authentication code
HN	Home Network
IBC	Identity Based Cryptography
ME	Mobile Equipment
MR	Measurement Report
PAIP	Protection area information provisioning
PKAT	Protection key agreement and transfer
PKC	Public Key Certificate
PKG	Private Key Generator
PKI	Public Key Infrastructure

(Continued)

(continued)

Abbreviation	Full name
RTT	Round trip time
SDR	Software Defined Radio
SEAF	Security Anchor Function
SI	System Information
SN	Serving Network
SON	Self-Organizing Network
SRKG	Share Root Key Group
TMSI	Temporary Mobile Subscriber Identity
UDM	Unified Data Management
UE	User Equipment
USIM	Universal Subscriber Identity Module

Appendix B Notations of BAN Logic

Notation	Description
$P\vert \equiv X$	P believes that the message X is true
$P \triangleleft X$	P receives the message X at any point in time
$P\vert \sim X$	P previously sent the message X
$P\vert \Rightarrow X$	P has jurisdiction over X
$\#(X)$	X is fresh
$P \overset{K}{\leftrightarrow} Q$	K is a secret key shared between P and Q
$P \overset{K}{\Leftrightarrow} Q$	K is a shared secret between P and Q.
$Expire_T$	X is encrypted with a key K
$\{X\}_K$	X is combined with Y
$X,\ \ Y$	P receives the message X at any point in time

Appendix C Rules of BAN Logic

Rule	Description
Message Meaning Rule (MM)	$\dfrac{P\vert \equiv P \overset{K}{\leftrightarrow} Q, \quad P \triangleleft \{X\}_K}{P\vert \equiv Q\vert \sim X}$ $\dfrac{P\vert \equiv P \overset{K}{\Leftrightarrow} Q, \quad P \triangleleft \langle X\rangle_K}{P\vert \equiv Q\vert \sim X}$

(Continued)

(continued)

Rule	Description
	$\frac{P\mid \equiv \overset{K}{\rightarrow} Q,\ \ P \triangleleft \{X\}_{K^{-1}}}{P\mid \equiv Q\mid \sim X}$
Nonce Verification Rule (NV)	$\frac{P\mid \equiv \#(X),\ \ P\mid \equiv Q\mid \sim X}{P\mid \equiv Q\mid \equiv X}$
Jurisdiction Rule (JR)	$\frac{P\mid \equiv Q\mid \Rightarrow X,\ \ P\mid \equiv Q\mid \equiv X}{P\mid \equiv X}$
Freshness Rule (FR)	$\frac{P\mid \equiv \#(X)}{P\mid \equiv \#(X,\ Y)}$
Decomposition Rule (DR)	$\frac{P \triangleleft (X,\ \ Y)}{P \triangleleft X}$
Belief Conjunction Rule (BC)	$\frac{P\mid \equiv X,\quad P\mid \equiv Y}{P\mid \equiv (X,\ Y)}$ $\frac{P\mid \equiv Q\mid \equiv (X,\ Y)}{P\mid \equiv Q\mid \equiv X}$ $\frac{P\mid \equiv Q\mid \sim (X,\ Y)}{P\mid \equiv Q\mid \sim X}$
Diffie-Hellman Rule (DH)	$\frac{P\mid \equiv Q\mid \sim \overset{g^Y}{\rightarrow} Q,\quad P\mid \equiv \overset{g^X}{\rightarrow} P}{P\mid \equiv P \overset{g^{XY}}{\leftrightarrow} Q}$ $\frac{P\mid \equiv Q\mid \sim \overset{g^Y}{\rightarrow} Q,\ \ P\mid \equiv \overset{g^X}{\rightarrow} P}{P\mid \equiv P \overset{g^{XY}}{\Leftrightarrow} Q}$