Leveraging Group Secret Sharing Technology for FD-RAN: A Lightweight AKA Mechanism

Ning Wang[†*], Jiacheng Chen[*], Jianbing Ni[‡], Liquan Chen[†], Haibo Zhou[§]
[†] School of Cyber Science and Engineering, Southeast University, Nanjing, China
[*] Department of Strategic and Advanced Interdisciplinary Research, Peng Cheng Laboratory, Shenzhen, China
[‡] Department of Electrical and Computer Engineering, Queen's University, Kingston, ON, Canada
[§] School of Electronic Science and Engineering, Nanjing University, Nanjing, China
Email: {230229207, lqchen}@seu.edu.cn, chenjch02@pcl.ac.cn, jianbing.ni@queensu.ca, haibozhou@nju.edu.cn

2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring) | 979-8-3503-8741-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/VTC2024-SPRING62846.2024.10683685

***Abstract*—With rapid advances in communication technology, a new access architecture of fully decoupled radio access network (FD-RAN) has been proposed. FD-RAN completely decouples the base station (BS) into uplink data base station (UBS), downlink data base station (DBS), and control base station (CBS). Different BSs handle the uplink and downlink data of the user plane, as well as control signaling, and facilitate communication needs through multi-BS cooperation. To ensure the security of multi-BS cooperation and user access, it becomes imperative to conduct key negotiations among multiple parties. However, as the number of simultaneously accessed BSs increases, the existing access security mechanism imposes excessive overhead in FD-RAN, compromising both access security and efficiency. Additionally, it becomes susceptible to distributed denial of service (DDoS) attacks launched by potential attackers. This paper introduces a lightweight authentication and key agreement (AKA) protocol based on secret value (m_i, n_i) sharing technology to negotiate multi-BS group communication keys, which ensures access security in FD-RAN. By leveraging interpolation polynomial and multi-party key negotiation, the proposed protocol achieves efficient and cost-effective key negotiation on both the user and BS sides, which mitigates the risk of man-in-the-middle (MitM) and DDoS attacks. Security analysis and further evaluation show that the proposed scheme can resist various known attacks, and guarantee the computational and communication efficiency of key negotiation within the FD-RAN context.**

***Index Terms*—FD-RAN AKA, multi-BS cooperation , access authentication, group key**

I. Introduction

To enhance communication performance, the next generation access network has been studied. Among them, fully decoupled radio access network (FD-RAN) [1], proposed by Yu et al., is a novel and effective scheme. As shown in Fig. 1, FD-RAN completely decouples the control plane and the user plane. Simultaneously, the base station (BS) is decoupled into the uplink data base station (UBS), the downlink data base station (DBS), and the control base station (CBS). Specifically, the UBS and the DBS handle uplink and downlink transmissions of user data respectively, while the CBS manages the interaction of control signaling with both users and data BSs. Leveraging multi-base station collaboration, flexible scheduling, and intelligent spectrum allocation, FD-RAN can ensure service quality and users' experience very well.

However, while FD-RAN introduces numerous advantages as a novel access architecture, it also presents new challenges.

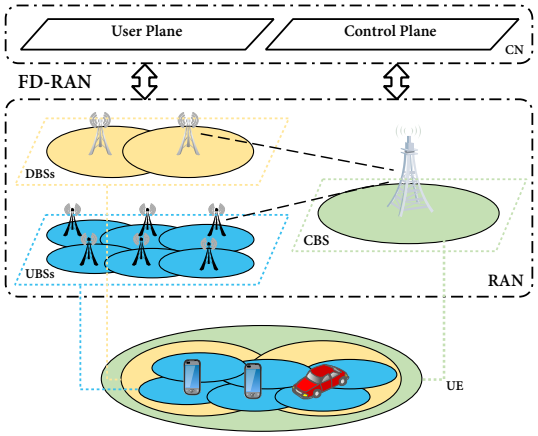


Fig. 1. FD-RAN Architecture

As depicted in Fig. 1, the FD-RAN framework results in an increased number of BSs serving the same user simultaneously, necessitating close collaboration among multiple BSs. Nevertheless, these BSs are situated externally, and with the complete decoupling of traditional BSs, their communication functions become dispersed and lose proximity to the core network (CN). External attackers could target or compromise these decoupled BSs, which poses a significant threat to the security of user data transmission and waste communication network resources. To address this and ensure the security of FD-RAN multi-BS cooperation, it is imperative to establish an efficient identification trust mechanism among the UBS, DBS, CBS, and the CN. This mechanism is crucial for safeguarding the security and integrity of the FD-RAN architecture.

Moreover, since its incredibility, simplex communication, and constrained computing capabilities, assistance from the CBS and the control plane becomes imperative when users access the data BS. This inherent challenge renders the existing fifth-generation (5G) mobile communication technology authentication and key agreement (AKA) [2] proposed by the 3rd generation partnership project (3GPP) group ill-suited for FD-RAN. Attempting to establish a multi-party trust relationship with 5G AKA would result in unsustainable authentication costs and if exploited by an attacker, could lead to distributed denial of service (DDoS) attacks. Consequently, FD-RAN

demands a more suitable AKA to ensure access security. The aforementioned mechanism must not only guarantee the safe and efficient cooperation between multi-BS and the CN but also ensure the security of user access to FD-RAN effectively.

To address analogous challenges, In [3], an anonymous switching authentication scheme for vehicle exhaust based on aggregate proxy signature technology is proposed. In [4], a group authentication scheme is proposed based on multiple signatures and aggregate message authentication codes (AMAC) technology. Employing the Chinese Remainder Theorem, a fast handover authentication protocol (FHAP) is introduced in [5]. The access authentication protocol proposed in [6] is mainly used to solve the problem of user anonymity and traceability. A lightweight group key negotiation mechanism using secret value sharing technology is proposed in [7] to enhance handover authentication. In [8], a comprehensive network roaming scheme is presented, spanning from 3GPP to worldwide interoperability for microwave access (WiMAX). This scheme encompasses handover authentication and secure channel establishment, accounting for the transition between different types of access points within the long term evolution (LTE) network. Two fixed-track handover authentication schemes tailored for group user handovers are proposed in [9], particularly applicable to fixed lines such as high-speed rail.

Although the above solutions contribute to security and authentication efficiency, they are not well suitable for FD-RAN multi-BS collaboration architecture, and therefore can not satisfy the security needs in FD-RAN.

In this paper, we employ a group key negotiation approach to establish an AKA mechanism among data BSs, the CN, and the user equipment (UE) in the FD-RAN architecture. The primary contributions of this work are outlined as follows:

- Utilizing a lightweight group key negotiation mechanism based on secret sharing technology, we construct interpolating polynomials for key negotiation between data BSs and the CN, and construct interpolating binomials to complete the FD-RAN AKA mechanism. This facilitates efficient and secure collaboration among multiple BSs, ensuring users' efficient and secure access to FD-RAN.
- Throughout the FD-RAN AKA mechanism, keys are independently generated at each end, mitigating the risk of man-in-the-middle (MitM) attacks. The implementation of 0-RTT access authentication between UE and data BSs reduces access overheads, enhancing both authentication and session efficiency and preventing DDoS attacks.
- Security analysis demonstrates that the proposed mechanism can resist numerous known attacks, while the formal BAN logic verification proves the security of it. Furthermore, a comprehensive analysis and comparison of the proposed security mechanism with existing schemes highlight that it is superior within the FD-RAN context.

The rest of this paper is organized as follows. In Section II, we describe the system model. The proposed scheme is explained in Section III. Security analysis and performance evaluation are completed in Section IV and Section V respectively. Finally, Section VI concludes the paper.

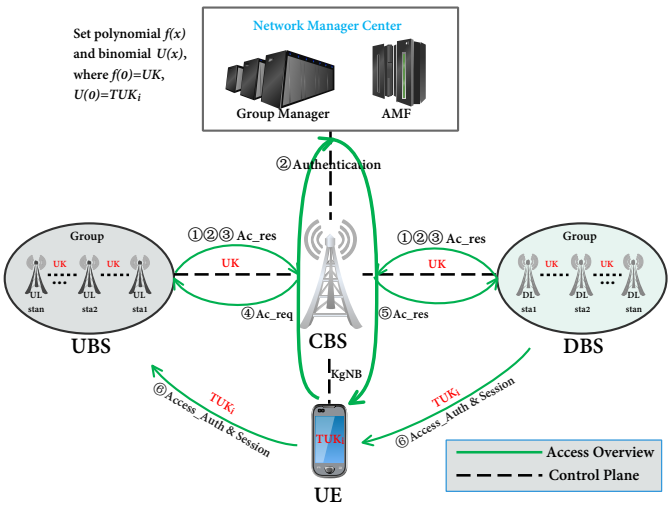


Fig. 2. System Model

II. System Model

This section describes the system model studied and the security assumptions for the corresponding entity.

The system model, depicted in Fig. 2, encompasses the following security entities: UBS, DBS, CBS, group manager (GM), network management center (NMC), and UE.

The following is security assumptions for the system model:

- This study is carried out in the static FD-RAN scenario.
- NMC&GM: It is assumed that the NMC and GM can not be destroyed by any opponent and are trusted. The GM is a trusted party integrated into the NMC.
- CBS: The CBS collects messages from data BS and forwards commands from the NMC to data BS. The CBS is completely trusted and it forwards signaling without error between data BS node and the NMC.
- Data BS: Data BS is untrusted, numerous, vulnerable, and have limited computing resources. Data BS may be impersonated by malicious adversaries, then trick other data BSs into providing access services to illegal users. There is no direct communication between data BSs and GM, no RRC channel is established, and signaling transmission can only be carried out through CBS forwarding. Therefore, establishing the trust relationship between data BSs and GM needs additional support.
- UE: The UE can be a variety of terminals with limited computing power, untrusted, and untrust data BSs.
- In addition, it is assumed that all data BSs can be attacked by viruses or even hijacked.

III. Proposed Scheme

In this section, an AKA scheme is proposed to achieve efficient security guarantee for FD-RAN multi-BS cooperation access security. It is described below:

The overall FD-RAN access flow is summarized in Fig. 3.

The process of accessing FD-RAN involves three steps. Step1 is the authentication between data BS and the CN.

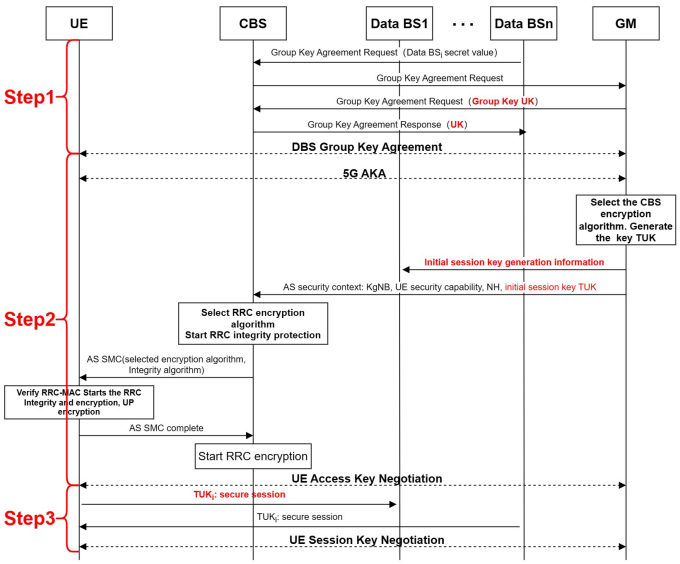


Fig. 3. FD-RAN Access Authentication Flow

Step2 is the authentication of UE accessing multi-BSs. Step3 is session key negotiation between user and data BS. For the convenience of description, the following are built with the UBS group as an example, which does not affect the presentation of the scheme. Specific description is as follows:

1) Step1: First, the data BS group completes group key negotiation with GM through CBS and obtains the key UK.

The group key negotiation scheme is shown in Fig. 2 ①,②,③. A group of data BSs in the same area can negotiate a shared group key with the help of CBS. Each m members in a group first send a set of values with randomly selected points and shared secret value (x_i, y_i) to the CBS nearby it. Each CBS then forwards the information it has collected to the GM securely. After receiving these m values, GM first selects a group key UK and lets $f(0) = UK$. Then, GM constructs an interpolating polynomial $f(x)$ of order M, regenerates m points on the polynomial $f(x)$, and returns them to each group member. These group members obtain the group key UK by recovering the polynomial, and use the key UK for group communication, thus establishing the trust relationship between the members in the group. All of them can interact securely through the key UK.

2) Step2: When UEs access FD-RAN, UE access CBS through the AKA mechanism first. At the same time, UE sends an key negotiation request to GM to negotiate the access security keys of UE and UBS.

At this stage, each legitimate UE_i is also authorized by the NMC, which acts as the group manager, sharing a secret value (m_i, n_i) with the NMC. These secret values will be stored in trusted hardware configured in the UE, and the data stored there can not be read by adversaries. The access key between the UE_i and UBS_i will be shared among the UE_i and UBS_i. The process is described as follows:

- Each UE_i with access needs first generates a random number R_{U_i} and timestamp ts_{u_i}, and then puts these data into the configured trusted security hardware. The trusted hardware module calculates $h(m_i, ID_{UE_i}, R_{U_i}, ts_{u_i})$ and feeds it back to the UE_i, where $h()$ is the hash function. Finally, UE_i uses CBS as the forward relay node to send the key negotiation request information to GM (sent by AKA mechanism):

$$GKA_{req}^{u_i} = \{h_i = h(m_i, ID_{UE_i}, R_{U_i}, ts_{u_i}), ID_{UE_i}, R_{U_i}, ts_{u_i}\}. \quad (1)$$

- After receiving the key negotiation request information $GKA_{req}^{u_i}$, GM first performs data source authentication and data integrity authentication on the received data: in this process, GM calculates $h^*(m_i, ID_{UE_i}, R_{U_i}, ts_{u_i})$ through the locally stored m_i and the received parameter $\{ID_{UE_i}, R_{U_i}, ts_{u_i}\}$, and compares whether h_i is equal to the calculated h^*. For the sake of description, assume that the UE_i authentication passes. After that, GM calculates the point $(m_i, n_i + R_{U_i})$ for the verified UE_i, generates t_s, assigns the UBS group to the user UE_i, derives the UBS group key UK, obtains

$$TUK_i = KDF(UK, ID_{UE_i}, ts_{new}), \quad (2)$$

and constructs binomial $U(x)$ through two points, namely $(0, TUK_i)$ and $(m_i, n_i + R_{U_i})$. Next, the GM selects point ${Q_i}^*$ on $U(x)$ for UE_i and calculates

$$Auth_{U_i} = h(TUK_i, ID_{UE_i}, ts_{new}, R_{U_i}, {Q_i}^*). \quad (3)$$

Finally, GM sends the key negotiation response message $\{Auth_{U_i}, ID_{UE_i}, ts_{new}, R_{U_i}, {Q_i}^*\}$ to the user UE_i, and

$$h_{new} = \{ENC_{UK}(ID_{UE_i}, ts_{new}), ts_{new}\} \quad (4)$$

to the corresponding UBS group. After the UBS in the group decrypts, the key TUK_i can be obtained.

- Once the response message is received, UE_i first calculates the point $(m_i, n_i + R_{U_i})$ through a trusted hardware module. Then, UE_i recovers the binomial $U(x)$ through the point $(m_i, n_i + R_{U_i})$ and the received point ${Q_i}^*$ to retrieve the initial session key $TUK_i = U(0)$. The UE_i then computes

$${Auth_{U_i}}^* = h(TUK_i, ID_{UE_i}, ts_{new}, R_{U_i}, {Q_i}^*) \quad (5)$$

and checks whether ${Auth_{U_i}}^*$ is the same as the received hash value $Auth_{U_i}$. If both values are the same, UE_i believes that the initial session key is valid and accepts it. Otherwise, UE_i stops key negotiation.

Through this process, UE_i and CBS complete the access authentication, confirm the trust relationship, and generate the key K_{gNB} to interact with CBS on the client side. Meanwhile, the key TUK_i is generated independently on the UE_i and UBS_i terminals. Next, when UE_i access UBS_i, UBS_i and UE_i can confirm each other's identities through TUK_i and completes the secure session.

The key TUK_i is used to complete access authentication and secure session between user UE_i and data BS group.

3) Step3:

- Different keys are required between UE_i and different UBS_i, which is accomplished by deriving the key TUK_i:

$$TUK_i{}^* = KDF(TUK_i, ID_{UE_i}, R_{AC_i}, ts_{new_u}), \quad (6)$$

where R_{AC_i} and ts_{new_u} are the new random numbers and timestamps generated by UE_i, respectively. For different UBS_i, the random number R_{AC_i} is different, so the key $TUK_i{}^*$ is different.

- UE_i sends access authentication requests and session information to UBS_i at the same time:

$$\begin{aligned} AC_{req} = \{&ENC_{TUK_i{}^*}(Message_u), ID_{UE_i}, \\ &ENC_{TUK_i}(R_{AC_i}, ts_{new_u}), h_{UE_i} = h(\\ &TUK_i{}^*, ID_{UE_i}, R_{AC_i}, ts_{new_u})\}. \end{aligned} \quad (7)$$

After receiving AC_{req} for the first time, UBS_i uses the key TUK_i and $ID_{UE_i}, R_{AC_i}, ts_{new_u}$ to derive the key $TUK_i{}^*$. By calculating

$$h^* = h(TUK_i{}^*, ID_{UE_i}, R_{AC_i}, ts_{new_u}) \quad (8)$$

and comparing whether h^* and h_{UE_i} are the same, data source authentication and data integrity authentication are carried out. After the authentication is successful, UBS_i use the key $TUK_i{}^*$ to decrypt the session information $Message_u$. In this way, UE_i completes UBS_i access authentication and secure sessions. In this process, access and session are performed simultaneously, and 0-RTT access authentication is implemented.

- After receiving the AC_{req} information of UE_i for the first time, UBS_i obtains the key $TUK_i{}^*$, and then uses the key to conduct a secure session with UE_i.

In summary, FD-RAN access security are guaranteed.

IV. Security Analysis

In this section, we analyze the security of the proposed scheme and verify the scheme by the formal model BAN logic.

A. Security Analysis:

- Mutual Authentication: The proposed scheme can realize the mutual authentication between UE_i and target data BS group. In the proposed scheme, only legitimate users will be able to upload or download data via data BSs. UBS_i verifies UE_i by checking the received $TUK_i{}^*$. Only legitimate users verified by GM can obtain the key TUK_i, so they can choose to complete the encryption, sending and decrypting of data by $TUK_i{}^*$ through key derivation. In addition, UE_i validates DBS_i by checking whether the received data is encrypted by TUK_i or its derived key. Because only legitimate DBS_i can use UK to decrypt h_{new} and get the initial session key TUK_i. Legitimate DBS_i can then choose to encrypt the data by key derivation and send it to UE_i. Therefore, the scheme can complete the mutual authentication between the user and the target data BS group.
- Resist Eavesdropping Attacks: The information generated by the key TUK_i is encrypted by GM using the data BS shared group key UK and encapsulated in h_{new}. Even if the attacker could intercept h_{new} with an eavesdropping attack, attacker would still not be able to get the key TUK_i because UK is unknown. In addition, the keys used to protect sensitive data are not transmitted over the communication link. Therefore, the proposed scheme can prevent attackers from launching eavesdropping attacks to obtain sensitive information.
- Resist Replay Attacks: Attackers always try to intercept messages and replay them further. However, when the timestamp value in the reply message is checked as invalid, attacker is still unable to successfully authenticate. In addition, the timestamp values cannot be modified and replaced because they are hashed to obtain key negotiation information $Auth_{U_i}$, h_{new}, and so on. Therefore, replay messages can be easily detected by checking the validity of timestamp and key negotiation information.
- Resist Man-in-the-Middle Attack: A MitM attacker cannot derive the initial session key TUK_i by eavesdropping on the public parameters of a wireless communication channel. Because TUK_i is derived based on key UK after mutual authentication is successful. Therefore, it is not feasible for an attacker to launch a MitM attack to invade an existing connection. In addition, an attacker cannot create the correct key negotiation request information without a shared secret value (x_i, y_i) or (m_i, n_i). Therefore, no one can impersonate a legitimate data BS or a legitimate UE.

B. BAN Logical Verification:

BAN logic is a formal model [10], which is widely used to analyze the security of authentication schemes. In this section, BAN logic is used to provide authentication proofs. Because the security process of UBS and DBS is the same, to simplify the description, the security of UE accessing UBS is verified in the following. Tab. I below describes some symbols and logical rules used in BAN logic analysis.

TABLE I
Symbols and Logical Rules

Symbole	**Description**
$P\mid\equiv X$	P trust X
$P \lhd X$	P can see X
$\sharp X$	X's id is fresh
$P\mid\sim X$	P mentioned X
$P \mid\Longrightarrow X$	P manage X
(X, Y)	X,Y is a part of (X,Y)
$\{X\}_K$	X is encrypted by key K
$P \overset{K}{\longleftrightarrow} Q$	P,Q communicate with the key K
Rules	**Formular**
R1.Message meaning rule	$\frac{P\mid\equiv P \overset{K}{\longleftrightarrow} Q, P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X}$
R2.Random verification rule	$\frac{P\mid\equiv \sharp(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
R3.Application of jurisdiction rule	$\frac{P\mid\equiv (Q\mid\Longrightarrow X), P\mid\equiv (Q\mid\equiv X)}{P\mid\equiv X}$

1) Safety Goals: The proposed protocol should meet the following safety goals:

- G1. $UBS_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- G2. $UBS_i| \equiv UE_i \mid\equiv UE_i \overset{TUK_i{}^*}{\longleftrightarrow} UBS_i$

2) Protocol Idealization: In order to facilitate derivation, the communication message of the proposed scheme is first converted into an idealized form, as follows:

- Message 1: $UE \longrightarrow GM$: Initial session key negotiation request information:

$$GM \triangleleft \{\{UE_i \overset{(m_i,n_i)}{\longleftrightarrow} GM, ID_{UE_i}, R_{U_i}, ts_{u_i}\}_h, ID_{UE_i}, R_{U_i}, ts_{u_i}\}. \quad (9)$$

- Message 2: $GM \longrightarrow UE_i$: Initial session key negotiation response message:

$$UE_i \triangleleft \{ID_{UE_i}, R_{U_i}, ts_{new}, {Q_i}^*, \{ID_{UE_i}, R_{U_i}, ts_{new}, {Q_i}^*, UE_i \overset{TUK_i}{\longleftrightarrow} TUK_i\ UBS_i\}_h\ \}. \quad (10)$$

- Message 3: $GM \longrightarrow UBS_i$: Transmission of initial session key generation information:

$$UBS_i \triangleleft \{\{ts_{new}, ID_{UE_i}, UBS_i \overset{TUK_i}{\longleftrightarrow} UE_i\}_{UK}\} \quad (11)$$

- Message 4: $UE_i \longrightarrow UBS_i$: Secure Access and Sessions:

$$UBS_i \triangleleft \{ID_{UE_i}, ts_{new_u}, R_{AC_i}, \{ID_{UE_i}, ts_{new_u}, R_{AC_i}, UBS_i \overset{TUK_i{}^*}{\longleftrightarrow} UE_i\}_{TUK_i}, \{Message_u\}_{TUK_i{}^*}\}. \quad (12)$$

3) Safety Assumption: In order to analyze the proposed scheme, the following assumptions are made about the initial state of the scheme:

- A1. $UE_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- A2. $UE_i| \equiv GM \overset{UK}{\longleftrightarrow} UBS_i$
- A3. $UBS_i| \equiv GM \overset{UK}{\longleftrightarrow} UBS_i$
- A4. $UBS_i| \equiv \sharp(ts_{new})$
- A5. $UBS_i| \equiv (UE_i/GM| \Longrightarrow UE_i \overset{TUK_i}{\longleftrightarrow} USB_i)$
- A6. $UE_i| \equiv \sharp(ts_{new})$
- A7. $UBS_i| \equiv \sharp(ts_{new_u})$
- A8. $GM| \equiv \sharp(ts_{u_i})$
- A9. $UE_i| \equiv \sharp(R_{U_i})$
- A10. $UBS_i| \equiv \sharp(R_{AC_i})$
- A.11 $GM| \equiv \sharp((m_i, n_i))$
- A.12 $GM| \equiv UE_i \overset{(m_i,n_i)}{\longleftrightarrow} GM$

4) BAN Logical Verification: Based on the idealized form of the message and hypothesis, the idealized scheme is analyzed. The following is the main proof procedure:

- According to message 1, message 2 and A1, A6, A12, applying R1, R2 yields:
  S1. $UE_i| \equiv UBS_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- According to message 3 and A3, applying R1 yields:
  S2. $UBS_i| \equiv GM| \sim \{ID_{UE_i}, ts_{new}, UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i\}$
- According to S2 and A4, applying R2 yields:
  S3. $UBS_i \mid\equiv GM| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- According to S3 and A5, applying R3 yields:
  S4. $UBS_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- According to message 4 and S4, applying R1 yields:
  S5. $UBS_i| \equiv UE_i| \sim \{ID_{UE_i}, R_{AC_i}, ts_{new_u}, UE_i \overset{TUK_i{}^*}{\longleftrightarrow} UBS_i\}$
- According to S5 and A7, A10, applying R2 yields:
  S6. $UBS_i| \equiv UE_i| \equiv UE_i \overset{TUK_i{}^*}{\longleftrightarrow} UBS_i$

Therefore, the above logic proves the access authentication security of the proposed scheme.

V. Performance Evaluation

In this section, the proposed authentication scheme will be compared with existing schemes in terms of computing overhead and communication overhead.

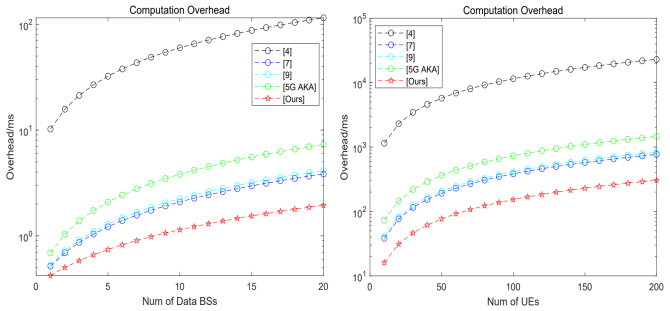
A. Computation Overhead

The cost of access authentication is defined as the time cost of the encryption operation involved in the proposed scheme. The time cost of using OpenSSL library for raw encryption operations on a 13th Gen Intel(R) Core(TM) i9-13900HX 2.20 GHz processor was investigated. According to the simulation results, the time cost of symmetric encryption/decryption operation $T_{sy} \approx 0.001ms$, the time cost of a one-way hash function $T_h \approx 0.019ms$ and the time cost of dot multiplication operation $T_M = 1.082ms$ are obtained. Tab. II compares the proposed authentication scheme with some existing work ([2], [4], [7] and [9]) in terms of the computational complexity of authentication delays. Among them, the total cost includes the cost of accessing CBS (5G AKA), which is $18T_h$, and the cost of accessing data BS for application schemes ([2], [4], [7] and [9]). As can be seen from Tab. II, the total time required for authentication in the proposed scheme is less than in the other schemes. This is because the operation used in our scheme is efficient (such as hash function), its operation cost is significantly less than other operations (such as dot multiplication), and our scheme is more suitable for FD-RAN.

TABLE II
Communication Overhead

Scheme/Cost	m **UE** n **DBS Access Authtication/ms**
[4]	$m * [21T_h + n * (5T_m + 5T_h + 2T_{sy}) + 4T_m]$
[7]	$m * [18T_h + n * (9T_h + 4T_{sy})]$
[9]	$m * [18T_h + n * 10T_h]$
5G AKA[2]	$m * [18T_h + n * (18T_h + 6T_{sy})]$
Ours	$m * [18T_h + n * (3T_h + 2T_{sy})] + n * (2T_{sy} + 2T_h)$

As shown in the Fig. 4: For a single UE, as the number of data BS providing services increases, the overhead generated during the access of each scheme is shown in Fig. 4(a). For 20 collaborative data BSs, as the number of connected UE increases, the overhead generated during the access of each scheme is shown in Fig. 4(b). Among them, the scheme in reference [4] costs much more than the other four because



(a) Multi-Data BSs Serve Single UE (b) 20 Data BSs Serve Multi-UEs

Fig. 4. Computation Overhead Comparison

of its complex operation. The remaining four schemes are mainly implemented through one-way hashing and symmetric encryption, which have low overhead. Among them, the scheme proposed by us has the lowest computational cost. As can be seen from Fig. 4, 5G AKA [2] scheme has higher computational overhead than the other three schemes, and in the FD-RAN multi-BS collaborative access scenario, 5G AKA [2] scheme cannot resist various attacks, such as DDoS attacks and MitM attacks. In addition, the 5G AKA [2] scenario does not establish a trust relationship within the data BS group. The authentication costs of the schemes in literature [7] and [9] are similar. In FD-RAN multi-BS collaborative access scenario, the computing costs are higher than our schemes. In addition, as will be analyzed next in the communication overhead, the proposed scheme also has a lower communication overhead in the FD-RAN. When the number of users is larger and the number of collaborative BSs is larger, the above advantages will be more obvious.

B. Communication Overhead

As for the communication cost, the size of the authentication message of the proposed scheme is evaluated and compared with some existing schemes. In order to better compare the communication overhead with existing schemes, we calculate the relevant parameters used in these schemes. Based on the size of all messages, as we can see in Tab. III that the communication overhead of the proposed scheme is lower than that of schemes in [2], [4], [7] and [9].

TABLE III
COMMUNICATION OVERHEAD

Option	Communication Overhead/bits
[4]	19456
[7]	4130
[9]	5376
5G AKA[2]	4520
Ours	3968

VI. CONCLUTION

In this paper, in the FD-RAN multi-BS cooperation scenario, we propose an AKA scheme to ensure multi-BS cooperation security and user access security. In FD-RAN, the proliferation of data BSs, coupled with the high cost of fiber connections and the lack of inherent trust between data BSs and other entities, underscores the need to establish a robust trust relationship among these components. To reduce access costs and avoid DDoS attacks, we cannot simply use the 5G AKA mechanism. Our scheme employs a lightweight group key negotiation protocol based on secret value sharing and share (x_i, y_i) and (m_i, n_i) secret value among data BSs, UE, and the CN respectively. This process facilitates key construction and the establishment of trust relationships between each ends. To further economize costs and ensure key security, the access and session keys between UE and data BSs are derived from data BS group keys. Security analysis demonstrates the scheme's resilience against known security attacks. Statistical analysis underscores the cost-saving advantages and efficient authentication capabilities inherent in the proposed scheme.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation Original Exploration Project of China under Grant 62250004, the Natural Science Foundation of China (NSFC) under Grant 62271244, Innovation and Entrepreneurship of Jiangsu Province High-level Talent Program, Summit of the Six Top Talents Program of Jiangsu Province, The Major Key Project of PCL, and The Basic and Frontier Research Project of PCL. *(Corresponding author: Haibo Zhou.)*

REFERENCES

[1] Q. Yu, H. Zhou, J. Chen, Y. Li, J. Jing, J. J. Zhao, B. Qian, and J. Wang, "A fully-decoupled ran architecture for 6G inspired by neurotransmission," *Journal of Communications and Information Networks*, vol. 4, no. 4, pp. 15–23, 2019.

[2] 3GPP, "5G; Security architecture and procedures for 5G system (3GPP Standard TS 33.501 V17.12.0 Rel.17)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 33.501, 2023.

[3] C. Lai and Z. Chen, "Group-based handover authentication for space-air-ground integrated vehicular networks," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[4] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for mtc within e-utran in lte-a networks," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7246–7251.

[5] Y. Yang, J. Cao, R. Ma, L. Cheng, L. Chen, B. Niu, and H. Li, "FHAP: Fast handover authentication protocol for high-speed mobile terminals in 5g satellite-terrestrial integrated networks," *IEEE Internet of Things Journal*, 2023.

[6] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5810–5822, 2022.

[7] K. Xue, W. Meng, H. Zhou, D. S. Wei, and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined space information network," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3673–3684, 2020.

[8] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3gpp and wimax networks," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 1011–1016.

[9] R. Ma, J. Cao, D. Feng, H. Li, and S. He, "FTGPHA: Fixed-trajectory group pre-handover authentication mechanism for mobile relays in 5G high-speed rail networks," *IEEE transactions on vehicular technology*, vol. 69, no. 2, pp. 2126–2140, 2019.

[10] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.