A Seamless Integration Solution for LoRaWAN Into 5G System

Hassan Jradi, Fabienne Nouvel, Abed Ellatif Samhat, Jean-Christophe Prévotet, Mohamad Mroue

A Seamless Integration Solution for LoRaWAN Into 5G System

Hassan Jradi[1,2], Fabienne Nouvel[1], Abed Ellatif Samhat[2], Jean-Christophe Prévotet[1], and Mohamad Mroue[2]

[1]Institut National des Sciences Appliquées de Rennes — IETR, Rennes, France.
[2]Lebanese University — Scientific Research Center in Engineering, Hadath, Lebanon.
[1]Email: firstname.lastname@insa-rennes.fr
[2]Email: samhat@ul.edu.lb, mohamad.mroue@ul.edu.lb

***Abstract*—The Internet of Things (IoT) has succeeded to be one of the important future communication technologies. The evolution of IoT has accelerated along with the emergence of 5G considered as a leading IoT service provider. In this context, the Low Power Wide Area Network (LPWAN) has recently attracted attention as it provides an impeccable infrastructure for massive Machine-Type Communications (mMTC). Long Range Wide Area Network (LoRaWAN) is one of the most adopted LPWAN technologies in the world. However, an efficient integration of LoRaWAN technology into the 5G System (5GS) is required. In this paper, we review briefly related work trying to integrate LoRaWAN into the 5GS. Then we present our solution for the integration and we detail the adopted network architecture. We propose new authentication methods based on the Extensible Authentication Protocol (EAP) providing secure access, and an adaptation function to attain seamless and efficient integration. In addition, we evaluate our solution in terms of performance and security. Moreover, a comparison of our solution with related work confirms the efficiency of our solution.**

***Index Terms*—Internet of Things, LoRaWAN, 5G, Security.**

I. Introduction

The Internet of Things (IoT) has actually become an important assistant in everyday life. 5G cellular networks or 5G technologies are the cutting-edge technologies in the provision of IoT services. 5G networks are part of the 3rd Generation Partnership Project (3GPP) — release 15 [1].

The 5G network architecture is divided into 5G Next Generation Radio Access Network (NG-RAN) [2], and 5G Core (5GC) Network [3]. The new architecture attracted attention since the design has shifted from a System Architecture Evolution (SAE) to a Service-Based Architecture (SBA) [4]. In SBA, the network services are divided into independent Network Functions (NFs) that are exposed by service providers and executed by service consumers. Along with the development of 5G networks and services, we noted the appearance of non-3GPP networks designed to provide IoT services such as LoRaWAN [5] and Sigfox [6].

LoRaWAN and Sigfox belong to Low Power Wide Area Network (LPWAN) technologies [7] where others exist such as DASH7 [8] and Wi-SUN [9]. LPWAN technologies are designed to provide a long communication range with low power consumption at a low data rate [10]. These characteristics are tailored for the massive Machine Type Communications (mMTC) application category of 5G [11]. However, the emerging LPWAN technology nowadays is LoRaWAN because the deployment of a LoRaWAN network is cost-effective since LoRaWAN uses the Industrial, Scientific, and Medical (ISM) frequency band which is unlicensed and free [12]. Currently, more than 166 LoRaWAN operators exist worldwide.

Motivation. Recent works [13], [14] have attempted to integrate the LoRaWAN network into the 5G System (5GS). This integration allows the operator to take advantage of both the simplicity and cost-efficiency of LoRaWAN, and the power and scalability features of 5G. Three advantages are picked up by making such an integration. First, 5G can provide free services for dedicated applications and areas covered by LoRaWAN gateways, similar to WiFi calling in LTE. Second, LoRaWAN can benefit from an SBA of 5G, which allows more devices to be managed more efficiently. Third, LoRaWAN can benefit from efficient mobility management through a dedicated 5G Network Function (NF).

Contribution. The main contributions of this paper are the following:

- Proposal of a network architecture achieving seamless integration.
- Proposal of authentication mechanisms that fulfills LoRaWAN join procedure and 5G authentication specifications (primary authentication and secondary authentication).
- Performance evaluation of the proposed solution as well as security evaluation.
- Comparison of the proposed solution with related work in terms of performance and security.

Paper organization. The rest of this paper is organized as follows. In Section II, we describe the basic concepts of LoRaWAN and 5G. In Section III, we discuss several related works for the integration of LoRaWAN into 5G. Our proposed solution for integration is introduced in Section IV, as well, the performance and the security evaluation are presented in Section V. A comparison of our solution with related work is detailed in Section VI, and Section VII concludes the paper.

II. Background

In this section, we review the network architecture, the identifiers and root keys used during the communication, and the authentication procedure for both LoRaWAN and 5G.

A. LoRaWAN

Network architecture. LoRaWAN architecture consists of five main elements as shown in Figure 1 and detailed below:

- End Device (ED): the sensor device sending the detected data to the network as an uplink message.
- Gateway (GW): the radio access point to which the ED is connected and acts as a pass-through element that forwards data in both directions.
- Network Server (NS): the core of LoRaWAN network responsible for data routing, data integrity validation, data rate adaptation and downlink GW selection. Regarding data routing, an uplink message sent by the ED on the radio link is received by one or more GWs will be forwarded on the TCP/IP links towards the NS. However, a downlink message sent by the NS on a unique TCP/IP link with the GW is forwarded to the ED on the radio link.
- Join Server (JS): an authentication server holding the ED identifiers and root keys. The JS has a main role in the authentication of EDs and it is not a main entity of a LoRaWAN operator since it may exist outside the network as a third-party entity. However, secure communication should be guaranteed between the JS and the NS, and between the JS and the AS. Moreover, the JS is responsible for deriving the necessary keys to protect the communication between the different entities after the authentication.
- Application Server (AS): a server responsible for receiving, processing and acknowledging the ED data.

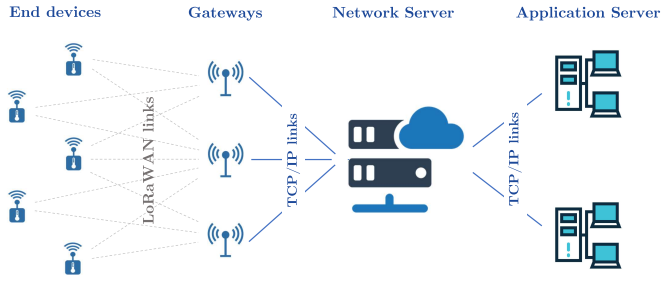

Fig. 1. LoRaWAN network architecture.

Identifiers and root keys. they are saved in the ED and in the JS. They are used in authentication, data protection and ED address generation.

- JoinEUI: the unique identifier – in IEEE EUI64 address space – of the AS to which the ED will send data.
- DevEUI: the unique identifier – in IEEE EUI64 address space – of the ED.
- NwkKey and AppKey: the root keys used to derive the session keys protecting the exchanged messages between ED $\longleftrightarrow$ NS, and between ED $\longleftrightarrow$ AS.

Device activation. it is achieved by the execution of the Join Procedure (JP). The current version of LoRaWAN (v1.1) [5] defines three JPs according to ED location: home network, passive roaming and active roaming procedures.

The JP in home network [15] is shown in Figure 2. 1) The ED sends a Join Request (JR) including JoinEUI, DevEUI, and a nonce DevNonce with MIC_{JR}. 2) The NS forwards the JR to the JS identified by the JoinEUI. 3) The JS derives the Network Session Keys (NwkSKeys) which are $SNwkSIntKey$ and $NwkSEncKey$, and the Application Session Key (AppSKey). 4) The JS sends the $AppSKey$ to the corresponding AS, the $NwkSKeys$ and join answer message to the NS. 5) The NS replies with a Join Accept (JA) message to the ED with MIC_{JA}. 6) The ED sends data to the AS protected using $AppSKey$ and routed by the NS. 7) If NS sends a command to the ED, it should be protected using the $NwkSKeys$.

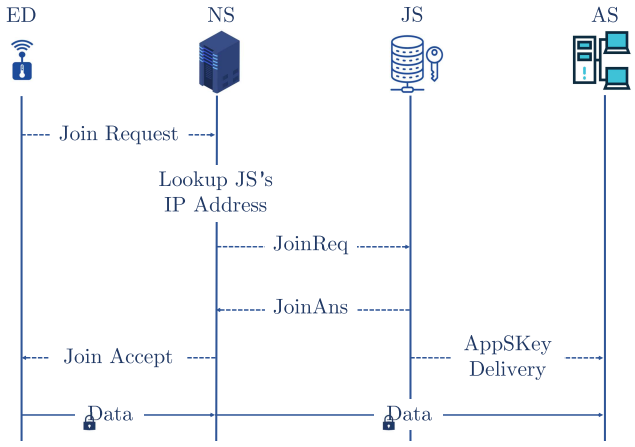

Fig. 2. LoRaWAN join procedure.

B. 5G

Network architecture. 5G architecture consists of the Next Generation Radio Access Network (NG-RAN) and the 5G Core (5GC) Network connected through the Next Generation (NG) interface as shown in Figure 3. One of the main features of the 5GC is being access-agnostic [16]. Thus, the RAN could implement any radio link technology on the condition to implement the NG interface between the RAN and the 5GC supporting the exchange of the Non-Access Stratum (NAS).

The main element in the NG-RAN is the gNodeB (gNB) responsible for radio resource management, IP header compression/decompression, routing of user-plane and control-plane data, and the transmission of paging messages, etc. NG-RAN can be further divided into gNB Central Unit (gNB-CU) and gNB Distributed Unit (gNB-DU). gNB functions are divided into higher-level functions aggregated in gNB-CU and lower-level functions aggregated in gNB-DU.

5GC has an Service-Based Architecture (SBA) where several Network Functions (NFs) compose the network. An NF notation is used in 5GC to indicate a set of programs or software that run on a cloud instead of running on dedicated hardware. The main NFs are the following:

- Access and Mobility Management Function (AMF): provides control-plane functions such as NAS signaling and AS security control.
- Security Anchor Function (SEAF): resides in the visited network in roaming case and acts as a relay during the authentication between the device and its home network.
- Authentication Server Function (AUSF): responsible for the execution of the authentication mechanism with the device trying to reach the network.

- Unified Data Management (UDM): responsible for the generation of credentials used during authentication including agreement keys, authentication vector and other device profile information.
- Session Management Function (SMF): responsible for the management of user-plane connectivity, and the session management for each device.
- User Plane Function (UPF): acts as a gateway towards the data network by routing and forwarding the data sent from the device to the ultimate destination.

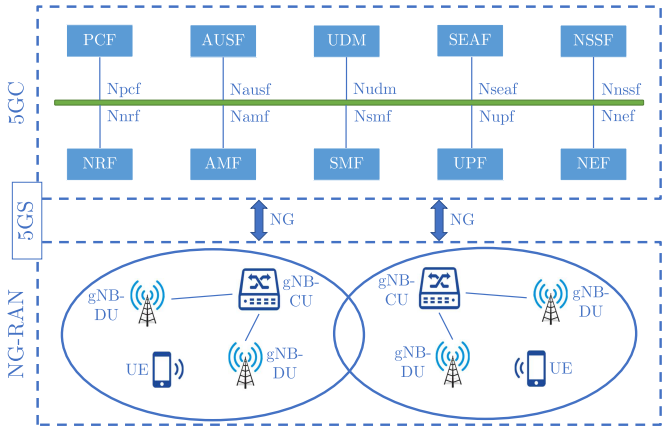

Fig. 3. 5G network architecture.

Identifiers and root keys. the main identifiers and keys used in the 5G network are the following:

- Subscription Permanent Identifier (SUPI): the unique and permanent subscription identifier assigned by the 5G network operator for each subscriber. This identifier should not be transmitted in plain text in any case over the radio link.
- Subscription Concealed Identifier (SUCI): since SUPI should not be transmitted in plain text, SUCI is the encrypted form of SUPI according to a protection scheme and using the home network public key.
- 5G Global Unique Temporary Identifier (5G-GUTI): a temporary identifier assigned by the AMF to the device after a successful authentication.
- Serving Network IDentifier (SNID): the identity of the network where the device is attached.
- Single Network Slice Selection Assistance Information (S-NSSAI): 5G network is designed for several purposes called slices like massive Machine Type Communications (mMTC), Ultra-high Reliability and Low Latency Communications (URLLC), and Enhanced Mobile Broadband (eMBB). S-NSSAI identifies the set of network slice functions used to serve the device ensuring a certain level of quality of service and providing a defined set of services.
- Protocol Data Unit (PDU) Session ID: an identifier for the session established between the device and the UPF and assigned by SMF after session establishment.
- Long-term secret key (K): the pre-shared key stored in the device and in the network (UDM NF). It is used to generate other keys like K_{AUSF}, K_{SEAF}, K_{AMF} and K_{NAS}.

Authentication and key agreement. 5G sets out two authentication procedures. The primary authentication is mandatory and required for device authentication with the 5GC. The secondary authentication is optional and aims to authenticate the device with the data network.

The primary authentication can be achieved using one of three mechanisms: 5G Authentication and Key Agreement (5G-AKA) [17], Improved Extensible Authentication Protocol (EAP) Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') [18], and EAP-TLS Authentication Protocol (EAP-TLS) [19].

EAP-AKA' is similar to 5G-AKA in terms of variables used to accomplish the authentication, however, EAP-AKA' uses EAP [20] messages including EAP-REQUEST, EAP-RESPONSE, EAP-SUCCESS, and EAP-FAILURE to deliver 5G-AKA variables. The EAP-AKA' authentication method is shown in Figure 4 and detailed below:

1) The User Equipment (UE) sends an authentication request containing SUCI to AMF/SEAF using N1 interface. The AMF/SEAF checks the validity and the home network of the requested SUCI, then forwards it to the AUSF of the home network along with the visited SNID through Nausf_UEAuthentication_AuthenticateRequest command. The AUSF forwards this request to UDM through Nudm_UEAuthentication_GetRequest.
2) UDM decrypts SUCI into SUPI then gets the corresponding UE policy and other information including the authentication method. Thereafter, UDM generates the authentication vector containing K_{AUSF}, RAND, AUTN, XRES, CK, IK and SUPI and sends it to AUSF through Nudm_UEAuthentication_GetResponse.
3) AUSF generates the EAP-REQUEST containing the AKA challenge to SEAF through Nausf_UEAuthentication_AuthenticateResponse. The SEAF forwards this message to UE using N1 interface.
4) The UE computes the response RES to the challenge (AUTN,RAND) and sends an authentication response with EAP-RESPONSE containing RES to SEAF using N1 interface. The SEAF forwards the response to AUSF using Nausf_UEAuthentication_AuthenticateRequest.
5) The AUSF validates RES according to XRES. If the validation passes, AUSF derives K_{SEAF}.
6) The AUSF sends EAP-SUCCESS to SEAF using Nausf_UEAuthentication_AuthenticateResponse containing K_{SEAF}. The SEAF gets its key K_{SEAF} and forwards the EAP-SUCCESS message to UE through N1 interface.
7) The AMF detects the success of the authentication, thus it derives a 5G-GUTI for the UE then sends it in the authentication response.
8) The UE derives control-plane keys including K_{AMF}, K_{NAS}. The SEAF provides AMF with K_{AMF} used to derive K_{NAS} for NAS protection.

In this way, the primary authentication is achieved where the UE and the 5GC agree upon control-plane keys.

On the other hand, the secondary authentication is completed with the data network through an authentication server which can be an Authentication, Authorization, and Accounting server (AAA server) using the EAP. At the end of this authentication, the device is associated with a new PDU

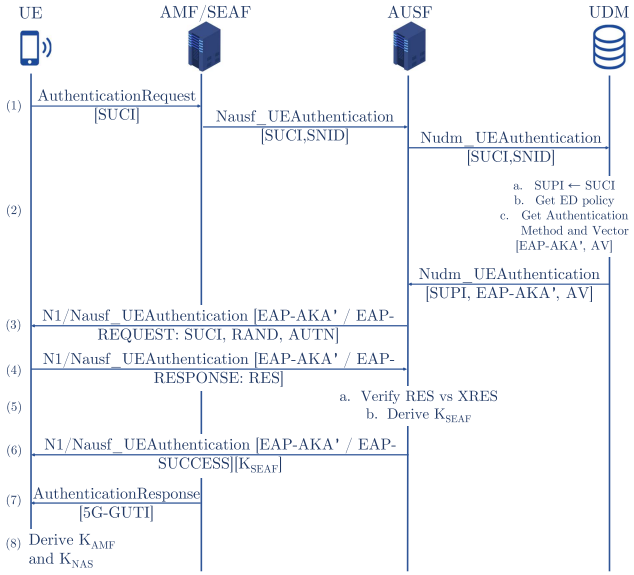

Fig. 4. 5G EAP-AKA' authentication method.

session managed by the corresponding SMF, and data are routed through the corresponding UPF.

In the next section, we present related work that studies the integration of LoRaWAN into 5GS.

III. Related Work

In this section, we present a work reviewing the main challenges of LPWAN integration into 5GS [21], and two integration proposals [13], [14].

A work that examines the challenges and the benefits of the integration of LPWANs and 5G was done by Sanchez-Gomez *et al.* [21]. This work presents the requirements for secure IoT applications and the 5G initiatives in the European Commission and in the research community. More importantly, it details the open challenges for the integration including:

- LPWAN heterogeneity due to the presence of several LPWAN communication technologies. The integration should examine the architecture, the protocol stack and the radio link characteristics to achieve seamless integration.
- Solution interoperability hence the integration solution should work consistently with the different LPWAN technologies.
- Mobility support since the device can move between several points of attachment and change its location and the access technology.
- Scalability since LPWANs deal with mMTC which involves a large number of connected devices concurrently.

A recent work done by Navarro-Ortiz *et al.* [14] endeavors to integrate LoRaWAN into 4G/5G system. The authors propose to leave the ED and the NS unmodified. But the LoRaWAN GW should behave as an eNodeB and a UE with a Universal Subscriber Identity Module (USIM) having the necessary network keys. The GW performs the connection establishment procedure on behalf of the ED since it has the necessary keys, and data are routed through the 4G/5G core network towards the NS, which in turn routes them to the correspondent AS. This work does not support mobility since the USIM is held by the GW, and if the ED moves to another GW, it cannot be authenticated.

Another work done by Torroglosa-Garcia *et al.* [13] proposes an integration solution that relies on the 5G network to perform authentication with LoRaWAN. The ED should have a valid USIM containing 5G keys in addition to LoRaWAN root keys. The ED tries to authenticate via LoRaWAN with the usual JP. If the procedure fails, the ED sends another JR containing 5G authentication parameters, which are processed by the 5GC as a 5G authentication request. Upon authentication success, the 5GC notifies the NS and sends the LoRaWAN session keys also generated by the ED. Thus the ED is authenticated in LoRaWAN through the 5GC and establishes a secure connection. This work fulfills mobility and scalability features, but LoRaWAN network stays a standalone network where the NS cannot benefit the 5GC NF.

As discussed above, few works tried to integrate LoRaWAN into 5GS. But several limitations exists in such works. However, the main objective of integration for LoRaWAN into 5G is to leverage the simplicity and cost-efficiency of LoRaWAN and the power and scalability features of 5G. We present a new integration solution that aims to achieve the following advantages:

- Highly scalable architecture: although LoRaWAN is characterized by its scalability and high network capacity, the use of an SBA core network is considered even more scalable. An SBA core network consisting of NFs interconnected through interfaces and manageable in a flexible way can achieve higher scalability. Thus, going from a simple LoRaWAN architecture to an SBA while conserving the main LPWAN functions and characteristics will increase LoRaWAN ability to serve mMTC applications.
- Dedicated network functionality: the integration of LoRaWAN into the 5GS makes it possible for LoRaWAN to benefit the existing NFs which were not implemented initially. For example, special algorithms that improve the mobility management like ED tracking and status monitoring may be implemented in the AMF, and others like roaming agreement and data buffering may be implemented in their corresponding NFs. Thus, an integrated LoRaWAN will benefit these implemented functions and exploit them to improve the performance and the QoS provided to the served EDs.
- Security and mobility features: one of the related work limitations was to provide security feature without mobility feature. However, an efficient and appropriate integration can achieve both features at the same time, which increases the adoption of the solution since mobility is an important requirement for several applications.
- Quasi-free services: if the RAN is formed by the LoRaWAN RAN, quasi-free services may be provided. This is possible for devices existing within the coverage of a LoRaWAN RAN and implementing LoRaWAN technology, similar to WiFi calling in LTE. Since LoRaWAN uses an unlicensed bandwidth for the communication between the EDs and GWs, the cost of using LoRaWAN is reduced to the cost of deployment of ED and GWs, where the high cost of owning

a licensed bandwidth is eliminated. Thus, in case an ED is using an LPWAN application requiring a small number of transmissions, it can benefit from such integration to send application data through the LoRaWAN RAN rather than sending them over a standard 5G RAN and occupying the licensed bandwidth.

However, achieving such an integration rises several challenges as described below where these challenges are addressed in our solution:

- Network compatibility challenge: the 5GC has a SBA consisting of several NFs that can be reached through their interfaces. However, the LoRaWAN architecture consists of the NS and the JS as the main core network entities. Thus, integrating NS and JS functionalities in the 5GC cannot be achieved simply by direct integration.
- Signaling compatibility challenge: in the 5GS, the control-plane communication between a UE and the 5GC is achieved through the NAS while it is ensured through the LoRaWAN Media Access Control (MAC) commands exchanged between the ED and the NS in LoRaWAN. The control-plane communication is a crucial communication in any network. However, a NAS message cannot be used for the control-plane communication between the ED and the 5GC since they will not be understood by the ED, and likewise for MAC commands that cannot be understood by the 5GC NFs. Thus, the integration solution should consider how to address the signaling compatibility challenge.
- Security challenge: an integration solution will lead to several security challenges like the authentication between the ED and the 5GS that should be ensured. In LoRaWAN and 5G standards, the authentication is achieved through the JP and the 5G authentication methods respectively. Thus, a compatibility challenge related to authentication should also be addressed in the integration solution.

Considering the advantages and the lack of work addressing the integration of LoRaWAN into the 5GS, we present in the next section our integration solution considering also the integration challenges.

IV. Proposed Solution

In this section, we present our proposed solution to integrate LoRaWAN into 5GS. We present first the design principles of our solution. Next, we describe the network architecture consisting of RAN and core network. Thereafter, we show the SUCI derivation scheme. Then we present our new authentication methods based on EAP which achieve primary and secondary authentication. After that, we detail the gNB-CU adaptation function used to support a seamless integration from LoRaWAN RAN into 5GC. Finally, we show how mobility is managed in several mobility scenarios.

A. Design principles

The following design principles are satisfied during the conception of our solution to achieve an efficient integration:

- Compatibility with LoRaWAN and 5G standards: in our solution, this compatibility is achieved at three levels. The first is at the network architecture level where the 5GC is adopted as the reference architecture and the LoRaWAN core network functionalities are divided over the corresponding NFs. The second is at the access procedure level where the LoRaWAN JP will be used as the network access procedure with the needed wrappings to be compatible with 5G primary and secondary authentication. The third is at the signaling and control level which are adapted to remain compatible with both standards by the use of an adaptation function.
- Network in network integration: this is related to the integration of NS and JS representing the main LoRaWAN core entities in the 5GC. Several concepts may be used to achieve this integration as the use of a connector entity that connects the LoRaWAN entities with the 5GC, or the use of the 5GC as a bridge network to connect the ED and LoRaWAN core entities. These concepts are simple to implement and can achieve integration, however, the integration will not be efficient as intended. For that, we use a more complex concept for integration that achieves superior performance where the concept used is to divide the functionalities performed by the NS and JS over the 5GC NFs.
- Seamless integration for devices: since the EDs in LoRaWAN have several constraints in terms of processing power and battery lifetime, we adopt a solution that avoids any additional procedures to be executed by the ED. Thus, the procedures involving the ED are the LoRaWAN procedures like the join procedure and data rate adaptation procedure. This is achieved thanks to the adaptation function responsible to provide translation of the signaling commands.
- Dedicated network slice: to complete the network in network integration design principle, we propose to assign a new network slice that allows to identify the required procedures in each NFs achieving the specified integration process.

B. Network architecture

Since we are integrating LoRaWAN into 5GS, the adopted network architecture is that of 5GS consisting of the RAN and the 5GC as shown in Figure 5. For that, the integration of LoRaWAN architecture into 5GS architecture is mainly done at two levels. The first is integrating LoRaWAN core network entities in the 5GC. The second is to make seamless integration of LoRaWAN RAN entities with the 5GC. Furthermore, although the data network is not considered a part of the 5GS, we present the principal entities involved during a communication scenario.

1) Network and join servers integration into 5GC: LoRaWAN NS and JS functions are distributed over 5GC NFs. The set of these NFs is identified using a new S-NSSAI named $SNSSAI_{LoRaWAN}$. In the following, we depict the operation of each 5GC NF in the LoRaWAN slice.

- UDM: in LoRaWAN, ED and JS pre-share $NwkKey$ and $AppKey$ which are used to derive $NwkSKeys$ and

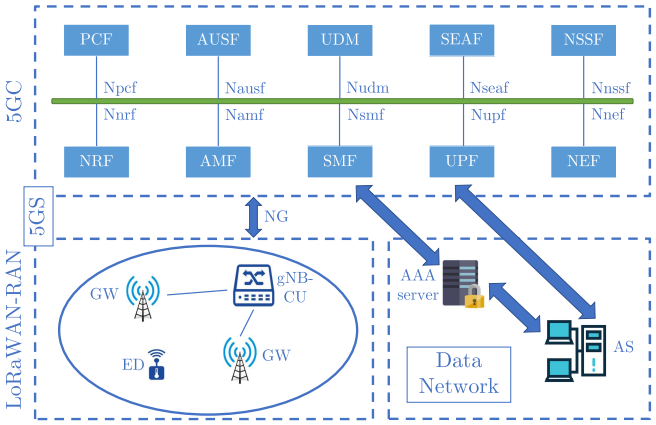

Fig. 5. The proposed network architecture for integration.

$AppSKey$. In our solution, we propose that the ED and UDM pre-share the long-term secret K which is saved in the ED USIM and in the UDM database respectively. The ED should possess a USIM since it is deployed in 5G network. K will be used to derive K_{AUSF} equivalent to $NwkKey$. We note that in LoRaWAN, $NwkKey$ is static (constant over time) whereas it is dynamic (changes over time) in our solution, which improves the security level. Hence, UDM holds ED profile including 1) SUPI derived from DevEUI to fulfill 5G standard (described later) 2) long-term secret key K 3) ED policy 4) authentication type set to EAP-LoRaWAN-CN (described later) 5) S-NSSAI set to $SNSSAI_{LoRaWAN}$.

- AUSF: gets K_{AUSF} and ED profile from UDM, then performs the primary authentication and key derivation based on EAP-LoRaWAN-CN authentication. In case of roaming, AUSF belongs to the home network domain.
- SEAF: has the main role in the primary authentication in case of roaming, thus it belongs to the visited network domain. SEAF gets K_{SEAF} derived by AUSF based on 5G standards, which is used to derive K_{AMF}.
- AMF: responsible for ED access and mobility management in the serving network. In our solution, we integrate LoRaWAN into 5G network, where ED realizes only LoRaWAN MAC commands, while a communication between an AMF/SMF and an ED is achieved through 5G Mobility Management (5GMM) / 5G Session Management (5GSM) NAS in 5G. Therefore, 5GMM/5GSM NAS messages sent from AMF/SMF to ED should be translated into LoRaWAN MAC commands. The translation mechanism will be performed by the gNB-CU adaptation function (described later).
- SMF: responsible for session management and contributes to the secondary authentication. In LoRaWAN, the ED establishes a session with the AS and protects the application data using the $AppSKey$. The LoRaWAN session context consists of the $AppSKey$, Uplink Frame Counter (FCntUp) and Application Uplink Frame Counter (AFCntUp) saved in the NS. In our solution, upon a session establishment with the 5G network, the SMF should store the LoRaWAN session context excluding the $AppSKey$. This key will be delivered by the AAA server to the AS after the secondary authentication using EAP-LoRaWAN-DN. Moreover, the SMF will assign an IP address and control a virtual PDU session established with the gNB-CU. The latter will handle the virtual PDU session instead of ED to maintain 5G compatibility through the adaptation function.
- UPF: in LoRaWAN, the routing is performed by the NS based on the ED Device Address (DevAddr) assigned after the session establishment. In our solution, the ED is assigned an IP address which is mapped to its DevAddr in the gNB-CU. When the ED sends uplink data, the gNB-CU gets its IP address based on DevAddr then sends it to UPF through the 5GC. Finally, UPF routes the data to the ultimate destination according to ED policy.

2) Gateways integration into 5G-RAN: the RAN consists of several gNBs, which are formed by gNB-DUs connected to gNB-CU as defined in 5G-RAN. The LoRaWAN GWs act as gNB-DUs and maintain their LoRaWAN function. The gNB-CU is responsible for LoRaWAN to 5G integration through the adaptation function described in Subsection IV-E.

3) Data network: consisting of AAA sever and AS as detailed below:

- AAA server: its role is to perform the secondary authentication to achieve secure access from ED to AS. AAA server has a database containing DevEUI with the correspondent $AppKey$. AAA server uses EAP-LoRaWAN-DN during secondary authentication then derives $AppSKey$ according to LoRaWAN key derivation scheme. In the end, $AppSKey$ is delivered to AS.
- Application Server (AS): responsible for the processing of data sent by ED. These data are protected using $AppSKey$ delivered by AAA server to AS after the secondary authentication.

C. SUCI derivation

USIM stores the SUPI that should not be exchanged as plain text on the air interface to conserve user anonymity. Thus, 5G standards propose to send SUCI instead of SUPI. SUCI contains SUPI encrypted in addition to several fields. In our solution, SUPI is equal to DevEUI, and SUCI is derived from it as shown in Figure 6 where:

SUCI Type	Home Network Identifier	Routing Indicator	Protection Scheme ID	Home Network Public Key ID	Scheme Output
LoRaWAN	LoRaWAN NetID	∀	0x00	0x00	DevEUI

Fig. 6. Derivation of SUCI from DevEUI.

- Home Network Identifier: set to LoRaWAN NetID where the ED is initially registered.
- Protection Scheme, Home Network Public Key ID, Scheme Output: since the DevEUI is sent in plain text in LoRaWAN, we can discard the protection and the public key where DevEUI is used as the scheme output. Note that the proposed fields could be adapted according to any future modification.

D. EAP-LoRaWAN authentication

Both LoRaWAN and 5G deploy their authentication mechanism to guarantee secure access from ED to the network. Nevertheless, integrating LoRaWAN into 5G requires either using one of the 5G authentication methods (5G-AKA, EAP-AKA', EAP-TLS), or inventing a new authentication method considering 5G standards and LoRaWAN JP at the same time.

In our solution, we choose the second approach and we propose two authentication methods based on EAP called LoRaWAN over EAP for Core Network (EAP-LoRaWAN-CN), and LoRaWAN over EAP for Data Network (EAP-LoRaWAN-DN). The load over the device is reduced since we are working with a LoRaWAN ED. This is due to the fact that the ED will only send and receive the JR and JA messages as in LoRaWAN JP, while the rest will be done by the gNB-CU on behalf of ED.

EAP-LoRaWAN-CN is used to achieve the primary authentication between ED and 5GC. The entities involved in this step are ED, gNB-CU, AMF, SEAF, AUSF, and UDM. EAP-LoRaWAN-CN is inspired by LoRaWAN JP, therefore the same parameters are exchanged and the LoRaWAN key derivation process is used to obtain the $NwkSKeys$. At the same time, we strive to take 5G standards into account.

At the other end, EAP-LoRaWAN-DN is used to achieve the secondary authentication between ED and the data network. The entities involved in this step are ED, gNB-CU, SMF, AAA server and AS. Upon the end of this step, the ED and AS get the $AppSKey$ needed for application data protection.

To start up with the access procedure, the ED sends LoRaWAN JR containing {JoinEUI, DevEUI, DevNonce, MIC_{JR} and MIC_{AAA}}. MIC_{JR} is the MIC defined in LoRaWAN JR and used in EAP-LoRaWAN-CN. However, the new MIC_{AAA} is used in EAP-LoRaWAN-DN authentication and calculated as follows:

$$MIC_{AAA} = aes128\_cmac(\textbf{AppKey},\ MHDR \mid JoinEUI \mid DevEUI \mid DevNonce)$$

This request is received by gNB-DU (LoRaWAN GW) and forwarded to gNB-CU as shown in Figure 7.

Fig. 7. Join request message at the beginning of the access procedure.

The steps of the primary and secondary authentication using EAP-LoRaWAN-CN and EAP-LoRaWAN-DN are shown in Figure 8 and 9 respectively.

Primary Authentication.

1) The gNB-CU saves ED JR and derives SUCI as detailed previously, then sends an authentication request to AMF through N2 interface containing SUCI.
2) The AMF forwards this request to AUSF using Nausf_UEAuthentication_AuthenticateRequest service containing also the SNID.
3) The AUSF forwards this request to UDM using Nudm_UEAuthentication_GetRequest service.
4) The UDM gets SUPI from SUCI according to the protection scheme. Then the UDM gets the ED policy and other information. Furthermore, the UDM derives K_{AUSF} from K according to 5G key derivation protocol.
5) The UDM replies to AUSF using Nudm_UEAuthentication_GetResponse service with SUPI, SUCI, the authentication type that should be used which is EAP-LoRaWAN-CN, and $K_{AUSF}(= NwkKey)$. In the following, AUSF takes the role of EAP-server, AMF/SEAF takes the role of authenticator and gNB-CU takes the role of peer.
6) The AUSF sends an EAP-REQUEST containing SUCI to gNB-CU using Nausf_UEAuthentication_AuthenticateResponse indicating the start of EAP authentication.
7) The gNB-CU replies with EAP-RESPONSE consisting of JR parameters (JoinEUI, DevEUI and DevNonce) sent by ED at the beginning with MIC_{JR}, in addition to a JoinNonce using Nausf_UEAuthentication_AuthenticateRequest.
8) The AUSF verifies MIC_{JR} using $NwkKey$. If the MIC is valid, then AUSF derives $NwkSKeys$ and K_{AMF}, then the AUSF generates JA parameters according to LoRaWAN specifications with the corresponding MIC_{JA} .
9) The AUSF sends the EAP-SUCCESS message to gNB-CU through AMF which is notified of the authentication success using Nausf_UEAuthentication_AuthenticateResponse.
10) Thus, the AMF gets K_{AMF} then derives K_{NAS} and 5G-GUTI.
11) The NwkSKeys and K_{NAS} are shared with gNB-CU to be able to perform the translation of NAS to LoRaWAN commands.

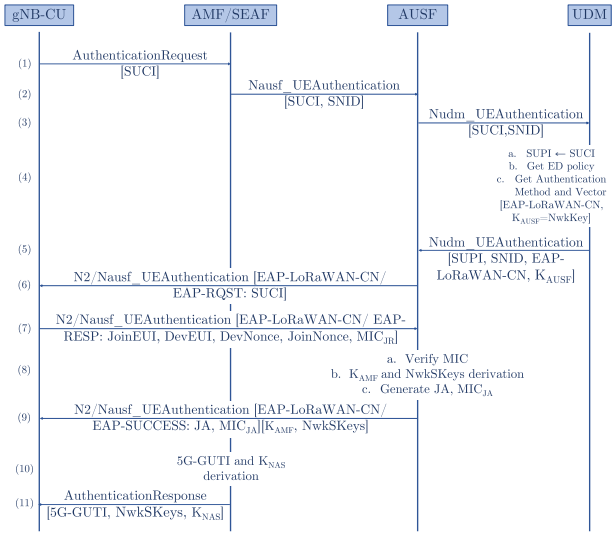

Fig. 8. The proposed primary authentication using EAP-LoRaWAN-CN.

Secondary Authentication.

1) The gNB-CU sends a PDU session establishment request to AMF containing {5G-GUTI and DevEUI} protected using

K_{NAS} and encapsulated into 5GSM NAS.
2) The AMF detects the 5GSM type of NAS, thus, the AMF decrypts it and forwards it to SMF using Nsmf_PDUSession_CreateRequest.
3) The SMF receives the session establishment request, thus it sends an authentication start flag containing DevEUI to AAA server residing in the data network. The SMF also holds a mapping between 5G-GUTI and DevEUI.
4) The AAA server starts the EAP-LoRaWAN-DN authentication by sending an EAP-REQUEST message to SMF containing the DevEUI. This request is forwarded by the SMF to the corresponding gNB-CU. In the following, AAA server takes the role of EAP-server, SMF takes the role of authenticator and gNB-CU takes the role of peer.
5) The gNB-CU sends an EAP-RESPONSE message containing the JR parameters with MIC_{AAA} and the saved JoinNonce used to derive the $AppSKey$.
6) The AAA server checks MIC_{AAA} using the pre-shared $AppKey$.
7) If the MIC is valid, the AAA server sends an EAP-SUCCESS message which indicates to SMF that the authentication has succeeded.
8) The SMF allocates the necessary session parameters including the IP address and sends an Namf_Communication_N1N2MessageTransfer to AMF to setup the uplink/downlink data path.
9) The AMF sends a PDU session establishment accept to gNB-CU with the 5G-GUTI and the other session parameters.

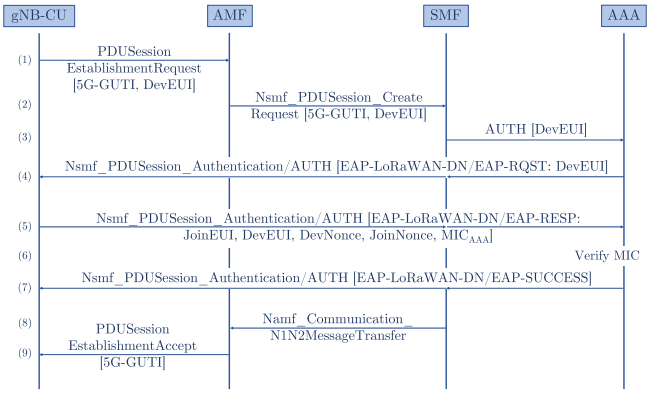

Fig. 9. The proposed secondary authentication using EAP-LoRaWAN-DN.

At the end of secondary authentication, the AAA server derives the $AppSKey$ and sends it to AS. Moreover, the gNB-CU replies to the ED with LoRaWAN JA containing {JoinNonce, Home_NetID, DevAddr, DL_Settings, RxDelay, CFList and MIC_{JA}} as shown in Figure 10. The ED derives the $AppSKey$ and configures its radio link interface based on the received parameters.

In this way, the ED is authenticated with the 5GC and AS and able to send/receive data securely.

E. gNB-CU adaptation function

In our solution, the ED physical layer is unchanged, thus LoRa modulation is still used where there is no need to support

Fig. 10. Join accept message at the end of the access procedure.

5G radio access technology. Also, the ED link layer is intact, where it still communicates using LoRaWAN MAC commands with the 5GC (substituting the NS). Besides, the control-plane communication between the ED and 5GC is managed through AMF and SMF using 5GMM and 5GSM NAS. Therefore, any downlink control-plane message sent from AMF or SMF to ED will not be understood by the ED since it realizes only LoRaWAN MAC commands, and vice versa for uplink LoRaWAN MAC commands. For that, we introduce our new function called the adaptation function implemented in gNB-CU node. This function is responsible for:

1) **Translation of 5GMM/5GSM NAS into LoRaWAN MAC commands and vice versa:** the main 5GMM NAS procedure messages that should be translated are: service request, primary authentication, security mode control, configuration update, and identification. The first three procedures are part of authentication achieved as explained previously using EAP-LoRaWAN-CN. The translation of the rest procedure messages is as follows:
   - Configuration update procedure: this procedure is translated according to the NAS message content into one of the following LoRaWAN commands: LinkCheck-Req/Ans, NewChannelReq/Ans, ReKeyInd/Conf, ForceRejoinRequest, RejoinParamSetupReq/Ans. The gNB-CU identifies the intended ED using the 5G-GUTI in the NAS message.
   - Identification procedure: this procedure is translated into DevStatusReq/Ans LoRaWAN commands, where the AMF asks the ED identity or status. The ED identity is the DevAddr translated into SUCI or 5G-GUTI in the gNB-CU. The status consists of ED related information such as battery level.

   The main 5GSM NAS procedure messages that should be translated are: session establishment and secondary authentication. These procedures are part of authentication achieved as explained in the previous subsection using EAP-LoRaWAN-DN.
2) **Handling of ED specific procedures:** three procedures are handled by gNB-CU on the ED behalf for two reasons: a) ED is not aware of the 5G parameters b) ED has battery and power consumption constraints. The three procedures are detailed below:
   - Registration Update (RU) procedure: for periodic RU, the gNB-CU launches a timer for each connected ED, when the timer elapses, gNB-CU sends a RU message to the AMF on ED behalf. For mobility RU, when the next gNB-CU receives uplink data sent from an ED, it tries to find the last serving gNB-CU (previous gNB-CU). When the next gNB-CU belongs to a tracking area

different from the previous gNB-CU tracking area, it sends a Mobility RU request to AMF on ED behalf, indicating the change of ED location and its radio access point. The ED context is sent from the previous to the next gNB-CU through the Xn or N2 interface.

- Session modification procedure: since the gNB-CU creates a virtual session for each ED, it is responsible to manage the session where the whole procedure is transparent to the ED. Moreover, the virtual session parameters are quasi-static since the gNB-CU has not the same ED dynamic behavior, thus this procedure is executed rarely. This procedure involves the tuning of parameters such as the maximum data rate and the quality of service.
- Session release procedure: this procedure comes after the RU procedure. When the ED moves from a previous to a next gNB-CU connected to AMF, it sends a Mobility RU to the previous gNB-CU. Thus, the latter should send a session release message to the SMF. Moreover, a new LoRaWAN session context is established through the next gNB-CU and SMF.

3) **Management of the radio links of the connected GWs based on the LoRaWAN protocol:** the gNB-CU is responsible for radio link management which is a pure LoRaWAN process previously performed by NS. The LoRaWAN MAC commands involved in this context are LinkADRReq/Ans, DutyCycleReq/Ans, RxParamSetupReq/Ans, NewChannelReq/Ans, RxTimingSetupReq/Ans, TxTimingSetupReq/Ans, DIChannelReq/Ans, ADRParamSetupReq/Ans, DeviceTimeReq/Ans. However, the gNB-DU, which is the GW, still acts as a relay for uplink and downlink messages as in LoRaWAN.

F. Mobility management

We focus on mobility management for three types of mobility that may occur in 5GS. The main parameters that can be changed in a mobile environment are the following:

- Radio link parameters including data rate, spreading factor, transmission and reception time window, etc.
- Session keys including K_{NAS} and $NwkSKeys$.
- Virtual PDU session including LoRaWAN session context, mapping between DevAddr and IP address, and other PDU session parameters.

The first type of mobility is the ED movement between two gNB-DU connected to the same gNB-CU, called intra-gNB-CU mobility. In this scenario, the radio link parameters change according to the new gNB-DU. However, the session keys are not modified since K_{NAS} changes whenever AMF changes and $NwkSKeys$ change whenever the ED changes the visited network domain. Moreover, the virtual PDU session is not affected since it is managed by the same gNB-CU. The ED is not required to perform any mobility related procedure.

The second type of mobility is the ED movement between two gNB-DUs connected to different gNB-CUs, called inter-gNB-CU mobility. In this scenario, the radio link parameters change according to the new gNB-DU. In addition, the virtual PDU session parameters should be sent from the previous to the next gNB-CU then updated. The session keys are not changed for the same previous reasons. The ED is not required to perform any mobility related procedure.

The third type of mobility is the ED movement between two gNB-CU connected to different AMFs, called N2-based mobility. A ForceRejoinRequest is sent to ED, thus ED starts the JP followed by the primary and secondary authentications.

TABLE I
LENGTH OF SIGNALING MESSAGES OF ACCESS PROCEDURES.

Method	Message	Description	Length
Join Procedure	JR	Join Request (ED-NS)	22
	HNSR	Home NS Request	8
	HNSA	Home NS Answer	3
	PR	Profile Request	8
	PA	Profile Answer	50
	HR	Handover Request	156
	JRq	Join Request (NS-JS)	62
	JAn	Join Answer (JS-NS)	64
	HA	Handover Answer	139
	JA	Join Accept (NS-ED)	16
	KD	AppSKey Delivery	20
	Total		**548**
5G EAP-AKA'	M1'	Authentication Request	17
	M2'	Nausf_UEAuthentication_Authenticate Request	18
	M3'	Nudm_UEAuthentication_Get Request	22
	M4'	Nudm_UEAuthentication_Get Response	88
	M5'	Nausf_UEAuthentication_Authenticate Response	44
	M6'	EAP-REQUEST	43
	M7'	EAP-RESPONSE	39
	M8'	Nausf_UEAuthentication_Authenticate Request	36
	M9'	EAP-SUCCESS	44
	M10'	Authentication Response	11
	Total		**362**
EAP-LoRaWAN-CN	M1	Authentication Request	17
	M2	Nausf_UEAuthentication_Authenticate Request	18
	M3	Nudm_UEAuthentication_Get Request	22
	M4	Nudm_UEAuthentication_Get Response	44
	M5	Nausf_UEAuthentication_Authenticate Response	36
	M6	EAP-REQUEST	39
	M7	EAP-RESPONSE	47
	M8	Nausf_UEAuthentication_Authenticate Request	36
	M9	EAP-SUCCESS	60
	M10	Authentication Response	43
	Total		**362**
EAP-LoRaWAN-DN	M11	PDU Session Establishment Request	23
	M12	Nsmf_PDUSession_Create Request	23
	M13	AUTH (SMF-AAA)	8
	M14	EAP-REQUEST	12
	M15	Nsmf_PDUSession_Authentication Command	23
	M16	Nsmf_PDUSession_Authentication Command	55
	M17	EAP-RESPONSE	44
	M18	EAP-SUCCESS	4
	M19	Nsmf_PDUSession_Authentication Complete	15
	M20	Namf_Communication_N1N2Message Transfer	10
	M21	PDU Session Establishment Accept	19
	Total		**236**

In this way, the ED gets the new radio link parameters, the new session keys and the next gNB-CU holds and manages the new virtual PDU session parameters.

V. Performance and Security Evaluation

In this section, we evaluate the performance of our solution according to the signaling overhead, the storage requirement and the authentication delay. Furthermore, we evaluate the security of the authentication mechanism according to several security issues.

A. Performance evaluation

1) Signaling overhead: an important metric that should be evaluated is the signaling overhead due to the use of messages exchanged between ED, gNB-CU and NFs. In our case, we consider that the message length (in Bytes) represents the signaling overhead. The length of each message used in LoRaWAN JP, 5G EAP-AKA', EAP-LoRaWAN-CN, and EAP-LoRaWAN-DN is calculated separately and shown in Table I.

We distinguish between two types of signaling messages. The first type represents the signaling messages sent over a radio link which can be a LoRaWAN radio link in case of LoRaWAN RAN. The second type represents the signaling messages sent over a direct link, like the signaling messages between NS and JS in LoRaWAN or between 5G NFs.

- The signaling overhead of LoRaWAN JP is equal to 548 Bytes where 38 Bytes are due to radio link messages (JR and JA), thus 510 Bytes are exchanged over a direct link.
- The signaling overhead of 5G EAP-AKA' is equal to 362 Bytes where 28 Bytes are due to radio link messages (M1' and M10'). We note that the signaling overhead of 5G EAP-AKA' should be accumulated with a secondary authentication signaling overhead in order to compare with other access procedures.
- In our solution, the signaling overhead of EAP-LoRaWAN-CN is equal to 362 Bytes and the signaling overhead of EAP-LoRaWAN-DN is equal to 236 Bytes, with a total of 598 Bytes, where any of these Bytes is due to radio link. However, JR and JA messages are sent before and after EAP-LoRaWAN-CN and EAP-LoRaWAN-DN messages. The length of JR and JA messages are 42 Bytes due to which is equal to 38 Bytes (as in default LoRaWAN) plus 4 Bytes for MIC_{AAA}.

Several factors like ED movement at high velocity and multi-path fading lead to hardness on the radio link resulting in data loss. Thus the probability of failure (p) of a radio link leads to additional signaling overhead since re-transmission is needed to recover lost data. The signaling overhead for each access procedure attempt per ED is shown in Table II and represented in Figure 11.

The results show that LoRaWAN JP has the lowest signaling overhead since LoRaWAN uses a network architecture simpler than that of 5G, resulting in less signaling. Our solution requires more signaling than EAP-AKA' (combined with a secondary authentication method) since LoRaWAN attributes are sent during EAP-LoRaWAN-CN and EAP-LoRaWAN-DN to be compatible with both 5G and LoRaWAN standards.

TABLE II
Signaling overhead of access procedures.

Access procedure	Signaling overhead
Join Procedure	$510 + \frac{38}{1-p}$
5G Primary and Secondary Authentication	$598 + \frac{28}{1-p}$
Our Solution	$598 + \frac{42}{1-p}$

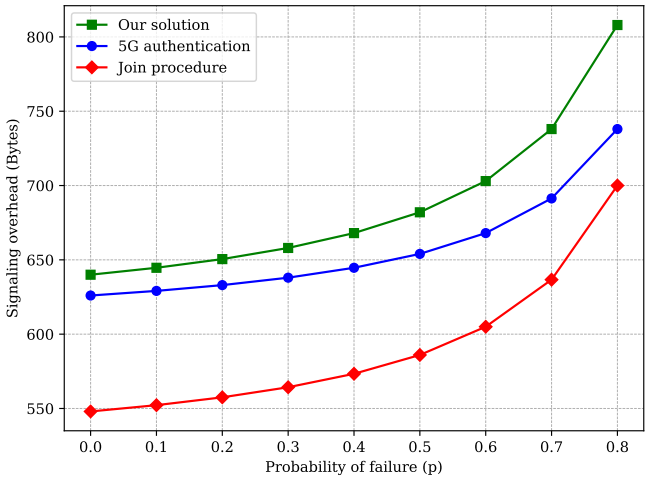

Fig. 11. Signaling overhead of access procedures in function of the probability of failure.

2) Storage requirement: The adaptation function leads to additional storage required by the gNB-CU. This is due to the session context of each ED managed by the gNB-CU. The session context consists of the following elements:

- The LoRaWAN session context.
- A mapping record between the 5G-GUTI, LoRaWAN DevAddr and IP address.
- The PDU session context of the session managed by the gNB-CU on the behalf of ED.
- The session keys including K_{NAS} and $NwkSKeys$.

In Table III, we detail the size of each parameter consisting the session context elements. The total size of storage needed for one ED management is equal to 122 Bytes. This value is compared with other solutions in the next section.

3) Authentication delay: Network Simulator 3 (NS-3) [22] is a discrete event network simulator that is widely used for research and education purposes where physical, link and network protocols are implemented in separate modules and can be combined or used to build new modules. NS-3 can simulate a wide range of network technologies, protocols, and applications, including wired and wireless networks, internet protocols, mobility models, and traffic models. It allows users to define network topologies, configure nodes, and run simulations to evaluate performance, analyze behavior, and compare different designs and algorithms. NS-3 supports a wide range of network protocols and technologies, including WiFi, WiMAX, and LTE. Moreover, NS-3 allows the simulation of mobile nodes using the mobility module and the visualization of captured data using graphs, 2D and 3D animations. NS-3 has a large and active community of users and developers who contribute to its development, provide support and documen-

TABLE III
STORAGE REQUIREMENT PER END DEVICE SESSION CONTEXT IN GNB-CU.

Element	Parameter	Size (Bytes)
LoRaWAN session context	FCntUp	4
	AFCntUp	4
	Total	**8**
Mapping record	5G-GUTI	10
	DevAddr	8
	IPv6 address	16
	Total	**34**
PDU session context	Identifier	1
	S-NSSAI	4
	DNN	8
	Session Type	1
	Mode	1
	UP Security	1
	Total	**16**
Device session keys	K_{NAS}	32
	SNwkSIntKey	16
	NwkSEncKey	16
	Total	**64**
Total	**122 Bytes**	

tation, and share their research and results of simulations.

Thus, we used NS-3 to create our new module called *lorawan-5g-integration*. The LoRaWAN module [23] is already created and can be used to test the radio link, however, the 5GC module is not built yet. For that, our module implements the main 5GC NFs including AMF, AUSF, SMF, UDM and UPF, as well as the main data network entities which are AAA sever and AS. In addition, we implement the gNB-CU to operate as explained in our solution. The implementation source codes can be found in [24].

The simulation scenario is made by an ED trying to enter a LoRaWAN network coverage. Thus it starts the access procedure by sending a JR to the network, then the primary and secondary authentications are achieved as explained before. Therefore, the link between ED and RAN is a LoRaWAN radio link, and RAN is connected to 5GC through NG interface. The metric monitored in the simulation is the Authentication Delay (AD) consisting of JR Delay (JRD), Primary Authentication Delay (PAD), Secondary Authentication Delay (SAD) and JA Delay (JAD), thus $AD = JRD + PAD + SAD + JAD$. JRD and JAD are the times needed for the JA and JR messages to be transmitted over the LoRaWAN link. JRD and JAD are impacted directly by the used Spreading Factor (SF). PAD and SAD are the times needed to complete the primary and secondary authentications. PAD and SAD are impacted mainly by the processing time needed to perform the operations, and by the characteristics of the links connecting the different NFs.

In our simulation, LoRaWAN bandwidth is equal to 125 kHz (supported in Europe and USA). We evaluate the performance of our solution according to LoRaWAN SF ranging from SF7 to SF12. Note that the higher the SF, the lower the data rate therefore the bigger the transmission delay. The results are shown in Figure 12. For a SF value of 10, 11 or 12, the dominant delays are JRD and JAD since the data rate is low, while PAD and SAD have minor contribution in AD. For these values of SF, the AD varies between 1182 ms and 3570 ms. However, for a SF value of 7, 8 or 9, JRD and JAD become low and comparable to PAD and SAD, where AD decreases to the range between 416 and 730 ms.

Comparing our solution to the default LoRaWAN JR, the two delays are approximately the same since we use the same number of messages on the radio link of LoRaWAN JP, where the transmission delay is the major contributor to the delay at low data rates.

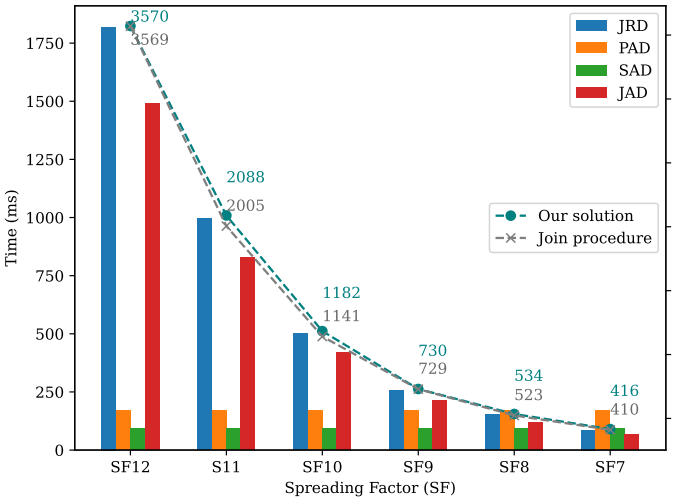

Fig. 12. Variation of evaluated metrics in function of spreading factors.

B. Security evaluation

1) Security analysis: The security of the proposed authentication methods is evaluated according to security issues detailed in our previous work [10]. We evaluate the security in order to prove that the integration solution including the new authentication methods achieves a secure integration solution.

- Device authentication: an ED should be authenticated with 5GC in roaming and non-roaming scenarios. This is guaranteed in 5G using one of the primary authentication methods (5G-AKA, EAP-AKA' and EAP-TLS). In roaming scenario, SEAF is responsible for the authentication of ED with the home network through AUSF. In our solution, the ED is authenticated with the 5GC using a new primary authentication method called EAP-LoRaWAN-CN involving SEAF and AUSF as required in 5G standards. Moreover, in case of the movement inside the same network coverage, i.e., intra-gNB-CU, inter-gNB-CU and N2-based mobility, the authentication and key agreement are managed as detailed in the previous section.
- Address squatting, spoofing and old address control: the address that should be protected from squatting and spoofing is the ED DevAddr. DevAddr is assigned by gNB-CU after the secondary authentication and sent in an encrypted and integrity-protected message. Moreover, data sent from ED to AS are encrypted using $AppSKey$, thus, an attacker trying to spoof the DevAddr could not send data to AS. In addition, LoRaWAN commands sent from ED to gNB-CU

are protected using $NwkSKeys$ preventing the spoofing of DevAddr.

- Mutual authentication: it implies that 5GC authenticates the ED, and ED authenticates 5GC. This is achieved using EAP-LoRaWAN-CN as detailed before, the 5GC authenticates the ED using the MIC_{JR} in the JR message, and the ED authenticates 5GC using the MIC_{JA} in the JA message. In addition, mutual authentication is achieved between the ED and the data network using MIC_{AAA} checked by the AAA server during the secondary authentication. Moreover, ED knows that an attacker cannot decrypt the data since they are encrypted using $AppSKey$ which guarantees secure data delivery.
- Key freshness: it ensures that the session keys are updated occasionally or on-demand to provide forward secrecy and to avoid the use of keys stolen by an attacker. Session keys are updated usually in case of mobility when the ED changes its radio access point. As detailed in our solution, the intra-gNB-CU and inter-gNB-CU do not require an update of $NwkSKeys$ or K_{NAS}. However, in N2-based mobility, $NwkSKeys$ and K_{NAS} are updated by sending a ForceRejoinRequest to the ED in order to re-authenticate with the 5GC.
- Context steal or alteration: The main context that should be protected is the PDU session context containing the LoRaWAN session context and other session parameters. This context is saved in the gNB-CU and in the SMF. As described before, this context is exchanged between the gNB-CU in case of mobility. However, it is not exchanged or disclosed to any entity which is not authorized to access.
- Replay attack: performed by the re-transmission of the initial attach request messages usually. However, the proposed authentication method resists this attack using the DevNonce field sent in the JR message. In addition, the JA message is protected from replay attack using JoinNonce field.

2) AVISPA evaluation: We use Automated Validation of Internet Security Protocols and Applications (AVISPA) [25] software to evaluate the security of our authentication methods. AVISPA is a software performing automated validation of internet security protocols.

An internet security protocol is implemented using the High-Level Protocol Specification Language (HLPSL) [26] where the entities involved in the protocol are defined. The messages exchanged between the entities are defined and each message is mapped to an entity state. When an entity receives a message matching the signature of a message defined in this entity, the defined actions are executed which can be a verification of the security parameters or a derivation of other secrets. In addition, after the executing of these actions, another message can be sent by this entity. The HLPSL implementation consists mainly of the definition of entities, the session combining these entities into one communication scenario, the environment where the secrets are declared, and the goals that should be ensured by the security protocol.

In our case, the implementation using AVISPA consists of the definition of each agent, the environment and the goals intended. In the environment, we declare five agents that will play the role of ED, gNB, AMF, SMF, AUSF, UDM, and AAA. In addition, we declare the keys used which are K and AppKey, as well as ED parameters like JoinEUI and DevEUI which are passed to the corresponding agents in the session declaration. Moreover, we declare a hash function, and the channels used to send and receive messages between the agents. Besides, we declare the intruder knowledge. In the end, we declare the session that aggregates these parameters in one communication scenario, while the rest of the code defines the exact operation of each agent according to authentication methods.

In the goal part, we focus mainly on the mutual authentication of ED with 5GC represented by the AUSF, and with the data network represented by the AAA server. The authentication with the 5GC is based on K and the derived NwkKey, while the authentication with the data network is based on AppKey, as defined in the rest of the implementation.

After running AVISPA for the implemented authentication methods, the output proves that it is safe as shown in Figure 13. The implementation source codes can be found in [27].

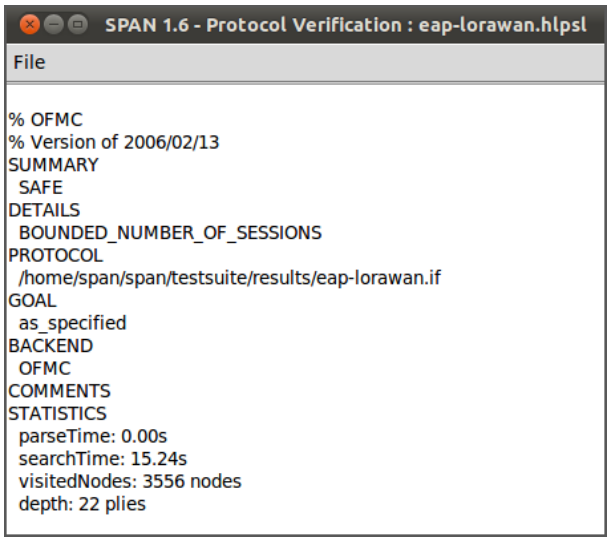

Fig. 13. Security evaluation using AVISPA.

VI. Comparison of Solutions

In this section, we compare our solution with related works proposed by Navarro-Ortiz *et al.* [14] and Torroglosa-Garcia *et al.* [13] according to the metrics evaluated in the previous section which are the signaling overhead, the storage requirement and the authentication delay. Moreover, we present the security features provided by each solution.

The related works did not evaluate completely their proposals according to our metrics, thus we studied them deeply to evaluate them according to our metrics.

A. Signaling overhead

In [14], the authentication method used is EAP-AKA' where the gNB performs a part of the authentication on behalf of ED, thus the signaling overhead is equal to EAP-AKA' with a secondary authentication to authenticate ED with the AS. In [13], two approaches are proposed, but we consider the

TABLE IV
COMPARISON BETWEEN THE PERFORMANCE OF OUR SOLUTION AND RELATED WORK.

Proposal	LoRaWAN standard [5]	Navarro-Ortiz *et al.* [14]	Torroglosa-Garcia *et al.* [13]	Our solution
Model type	Default	Network-Based	Host-Based	Network-Based
Adapted approach		LoRaWAN GW as 5G gNB	5G keys in ED	C-RAN & EAP
Mobility support	Yes	No	Yes	Yes
Signaling overhead	548 → 700	610 → 722	738 → 1170	640 → 808
Storage requirement	N/A	114 Bytes	48 Bytes	122 Bytes
Authentication delay	410 ms	792 ms	733 ms	416 ms

default case where an ED does not have an active 5G radio link. In this case, a JR re-transmission is needed. Moreover, two new services are defined in the UDM and accessed by JS to complete the authentication. The signaling overhead of the three solutions are shown in Table IV.

B. Storage requirement

In [14], the LoRaWAN GW holds a USIM containing the long-term secret K and acts as a gNB, thus GW should hold a session context consisting of a mapping record, a PDU session context and the derived session keys. In [13], the ED stores an additional JoinEUI, SUPI and long-term secret K to perform the alternate authentication using the 5G network. The storage requirements of the three solutions are shown in Table IV.

C. Authentication delay

In [14], the AD is evaluated through an experimental testbed using The Things Network (TTN) [28] where the results show that AD is approximately 792 ms assuming a bandwidth of 500 kHz and SF equals 7. In [13], a regular LoRaWAN JP is needed for the authentication preceded by a failed LoRaWAN JR attempt, thus the AD is greater than LoRaWAN JP AD. For a bandwidth of 250 kHz and SF equals 7, the AD is approximately 733 ms. The AD of the three solutions are shown in Table IV.

D. Security comparison

We evaluate the security of [13], [14] according to the security issues investigated in our previous work [10]. The comparison of these solutions is summarized in V.

- Device authentication: the authors in [14] proposed an access procedure replacing the LoRaWAN JP providing device authentication. However, the authentication cannot be achieved outside the location of the ED where it is considered an immobile ED, and can establish a connection with only one eNodeB. In [13], the authors propose an alternative way to provide LoRaWAN authentication using 5G network which support also authentication in case of roaming.
- Address squatting, spoofing and old address control: these security issues are not applicable in [14] since the ED is considered immobile. In [13], address squatting and spoofing are prevented since the DevAddr is assigned by the NS after each authentication success, and old address control is prevented since any packet sent from an ED is encrypted using the corresponding AppSKey mapped to DevEUI.
- Mutual authentication: this security feature is not achieved in [14] since the ED cannot authenticate the 4G/5G network. The authors propose that the eNodeB holds USIM containing 4G/5G credentials are not saved in the ED, thus it is not possible to authenticate the 4G/5G network. However, the authentication between the ED and the NS is achieved. In [13], mutual authentication between the ED and the NS is achieved although an alternative to LoRaWAN JP is used.
- Key freshness: after a successful authentication in [14], the ED and the NS derive the session keys according to LoRaWAN key derivation scheme. However, as the ED is immobile, the session keys are changed rarely and key freshness is not ensured. In [13], the session keys are also derived according to LoRaWAN key derivation scheme and are updated regularly according to the ED movement.
- Context steal or alteration: in [14], the context is not transferred from an eNodeB to another one since the ED is immobile, thus this security issue is not considered. In [13], the context is saved according to 5G and LoRaWAN standards thus it is considered secure.
- Replay attack: this security issues is prevented in the two solutions using LoRaWAN nonce fields employed in the JP, which are DevNonce and JoinNonce.

As a result, our solution provides competitive results in terms of performance, where we achieve a good signaling overhead, an acceptable storage requirement and the best authentication delay. At the same time, our solution ensures secure access along with additional security features.

VII. CONCLUSION

In this paper, we proposed a new solution for the integration of LoRaWAN into 5GS. We proposed a network architecture where the RAN is the LoRaWAN RAN, and the core network is based on 5GC. In addition, we proposed two authentication methods called EAP-LoRaWAN-CN and EAP-LoRaWAN-DN to achieve primary and secondary authentication. Moreover, the gNB-CU is supposed to perform an adaptation function to achieve seamless integration. The evaluation of our solution shows that it provides good performance, security features, and competitive results with related works.

REFERENCES

[1] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5g evolution: A view on 5g cellular technology beyond 3gpp release 15," *IEEE access*, vol. 7, pp. 127 639–127 651, 2019.

[2] S. Ahmadi, *5G NR: Architecture, technology, implementation, and operation of 3GPP new radio standards*. Academic Press, 2019.

TABLE V
SECURITY FEATURES PROVIDED BY OUR SOLUTION AND RELATED WORK.

	[14]	[13]	Our solution
Device authentication	✓	✓	✓
Address squatting and spoofing		✓	✓
Old address control		✓	✓
Mutual authentication		✓	✓
Key freshness		✓	✓
Context alteration		✓	✓
Replay attack	✓	✓	✓

[3] S. Rommer, P. Hedman, M. Olsson, L. Frid, S. Sultana, and C. Mulligan, *5G Core Networks: Powering Digitalization*. Academic Press, 2019.

[4] G. Brown, "Service-based architecture for 5g core networks," *Huawei White Paper*, vol. 1, 2017.

[5] N. Sornin and A. Yegin, "Lorawan 1.1 specification," *LoRa Alliance*, 2017.

[6] A. Lavric, A. I. Petrariu, and V. Popa, "Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions," *IEEE Access*, vol. 7, pp. 35 816–35 825, 2019.

[7] W. Ayoub, F. Nouvel, A. E. Samhat, M. Mroue, and J.-C. Prevotet, "Mobility management with session continuity during handover in lpwan," *IEEE internet of things journal*, vol. 7, no. 8, pp. 6686–6703, 2020.

[8] W. Ayoub, F. Nouvel, A. E. Samhat, J.-C. Prevotet, and M. Mroue, "Overview and measurement of mobility in dash7," in *2018 25th International Conference on Telecommunications (ICT)*, IEEE, 2018, pp. 532–536.

[9] P. Beecher, *Wi-sun alliance*, 2016.

[10] H. Jradi, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Overview of the mobility related security challenges in lpwans," *Computer Networks*, vol. 186, p. 107 761, 2021.

[11] Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub, "Toward massive machine type cellular communications," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 120–128, 2016.

[12] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2018.

[13] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe, and A. Skarmeta, "Enabling roaming across heterogeneous iot wireless networks: Lorawan meets 5g," *IEEE Access*, vol. 8, pp. 103 164–103 180, 2020.

[14] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of lorawan and 4g/5g for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.

[15] N. Sornin and A. Yegin, "Lorawan backend interfaces 1.0 specification," *LoRa Alliance*, 2017.

[16] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5g security in 3gpp," in *2017 IEEE conference on standards for communications and networking (CSCN)*, IEEE, 2017, pp. 181–186.

[17] ETSI, "Security architecture and procedures for 5g system," Sophia Antipolis, France, Tech. Rep. TS 33.501 V16.3.0, 2020.

[18] J. Arkko and H. Haverinen, *Extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka)*, RFC 4187, Jan. 2006.

[19] D. Simon, B. Aboba, and R. Hurst, *The eap-tls authentication protocol*, RFC 5216, Mar. 2008.

[20] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible authentication protocol (eap)*, RFC 3748, Jun. 2004.

[21] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Sanchez-Iborra, *et al.*, "Integrating lpwan technologies in the 5g ecosystem: A survey on security challenges and solutions," *IEEE Access*, 2020.

[22] *Network simulator 3*, May 2022. [Online]. Available: nsnam.org.

[23] *Lorawan ns-3 module*, Jan. 2022. [Online]. Available: github.com/signetlabdei/lorawan.

[24] *Lorawan-5g-integration ns-3 module*, May 2022. [Online]. Available: github.com/HassanJradi/lorawan-5g-integration.

[25] A. Armando, D. Basin, Y. Boichut, *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International Conference on Computer Aided Verification*, Springer, 2005, pp. 281–285.

[26] D. Von Oheimb, "The high-level protocol specification language hlpsl developed in the eu project avispa," in *Proceedings of APPSEM 2005 workshop*, APPSEM'05, Tallinn, Estonia, 2005, pp. 1–17.

[27] *Avispa hlpsl implementation*, Oct. 2021. [Online]. Available: github.com/HassanJradi/avispa.

[28] *The things network*, Mar. 2021. [Online]. Available: thethingsnetwork.org.