IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 10, 2020, accepted November 18, 2020, date of publication November 27, 2020,
date of current version December 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3041057

Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions

JESUS SANCHEZ-GOMEZ[1], DAN GARCÍA CARRILLO[2], RAMON SANCHEZ-IBORRA[1], JOSÉ L. HERNÁNDEZ-RAMOS[3], JORGE GRANJAL[4], (Member, IEEE), RAFAEL MARIN-PEREZ[2], AND MIGUEL A. ZAMORA-IZQUIERDO[1]

[1]Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain
[2]Department of Research and Innovation, Odin Solutions, 30820 Murcia, Spain
[3]European Commission, Joint Research Centre, 21027 Ispra, Italy
[4]Centre for Informatics and Systems, University of Coimbra, 3030-290 Coimbra, Portugal

Corresponding author: Ramon Sanchez-Iborra (ramonsanchez@um.es)

This work was supported in part by the Spanish Ministry of Science, Innovation and Universities (all with European Regional Development Fund (ERDF) funds) through the projects PERSEIDES under Grant TIN2017-86885-R, GUARDIAN under Grant TSI-100110-2019-20, and 5GHuerta under Grant EQC2019-006364-P; in part by the Seneca Foundation in Murcia Region under FPI Grant 20751/FPI/18; in part by the Industrial Doctorate from Ministerio de Economía y Empresa (MINECO) under Grant DI-16-08432; in part by PEANA under Grant UNMU13-2E-2536; and in part by the European Commission through the INSPIRE-5Gplus Project under Grant 871808, the Plug-n-Harvest Project under Grant 768735, the SerIoT Project under Grant 780139, the Fed4IoT Project under Grant 814918, the EU IoTrust Project under Grant 825618, the PHOENIX Project under Grant 893079, and the PRECEPT Project under Grant 958284.

ABSTRACT The convergence of the Internet of Things (IoT) and 5G will open a range of opportunities for the deployment of enhanced sensing, actuating and interactive systems as well as the development of novel services and applications in a plethora of fields. Given the processing and communication limitations of both IoT devices and the most novel IoT transmission technologies, namely, Low Power Wide Area Network (LPWAN), there are notable concerns regarding certain security issues to be overcome in order to achieve a successful integration of LPWAN systems within 5G architectures. In this survey work, we analyze the main security characteristics of LPWANs, specially focusing on network access, and contrast them with 5G security requirements and procedures. Besides, we present a comprehensive review and analysis of research works proposing security solutions for the 5G-LPWAN integration. Finally, we explore open issues and challenges in the field and draw future research directions. From our analysis, it is evident that many efforts are being devoted from the academia, industry and Standards Developing Organizations (SDOs) for achieving the desired confluence of IoT and 5G worlds. We envision a successful integration of both ecosystems by exploiting novel lightweight security schemes addressing the stringent security requirements of 5G while being assumable by constrained IoT devices.

INDEX TERMS 5G, Internet of Things (IoT), low-power wide-area network (LPWAN), security.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized our lives as it has paved the way for a plethora of applications and services never imagined few time ago. Undoubtedly, the IoT ecosystem will be integrated as part of the upcoming 5G paradigm [1]. Before the final development and deployment of these complex systems, a lot of effort is being devoted to the security aspects of the novel 5G architecture. It is envisioned that by the convergence of these technologies our daily life will be almost continuously connected, hence several challenges related to security and privacy emerge [2].

Most of the new wave of IoT services will be based on autonomous end-devices (EDs), which perform specific tasks in an unsupervised way, i.e., adopting a Machine-type Communication (MTC) approach [3]. These elements usually gain connectivity through wireless network technologies, thus enabling their deployment in remote and wide areas.

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

TABLE 1. Contribution comparison with related survey works.

Topic\Work	[1]	[2]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	This work
NB-IoT – 5G integration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
non-3GPP LPWAN – 5G integration	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
LPWAN communication security requirements	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes
IoT use-case security requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LPWAN security research	No	No	No	No	No	No	No	No	No	No	No	Yes
International initiatives	No	No	No	No	No	No	No	Yes	No	No	No	Yes
Standardisation efforts	Yes	No	Yes	Yes	No	No	No	Yes	No	No	No	Yes

Due to the constrained features of both EDs and typical IoT wireless technologies, the security aspects of these networks are not as robust as in traditional non-constrained architectures, consequently opening a door for potential malicious attacks focused on both the end-nodes and the core network.

One of the wireless technologies that is gaining great relevance for enabling novel IoT applications is Low Power Wide Are Network (LPWAN) [4]. The most prominent characteristics of these wireless communication solutions are i) long coverage range of over 10 km, ii) very low power consumption of EDs, and iii) great scalability. All of them are highly beneficial in IoT scenarios. However, these features are reached at the expense of reducing the number of daily transmissions and the size of the transmitted messages. Clearly, both restrictions severely harm the security capabilities of these wireless links that, as mentioned above, need to be protected for avoiding attacks of different nature.

The goal of this paper is to analyze the main security issues of LPWAN technologies that must be addressed, and their implications for integrating LPWAN networks in the 5G ecosystem. In fact, during recent years, there has been a constant and steady increase in the volume of publications about 5G security and LPWAN as presented in Fig. 1, which shows the yearly publications' volume extracted from Scopus,[1] a major academic abstract and citation index database. The covered time period goes from 1st January 2014 to 31st December 2019. The search returned 1536 publications during the 2018–2019 period regarding "5G Security" and "LPWAN" topics. This review analysis evidences the great interest in 5G and LPWAN ecosystems as well as in their potential convergence [5]. However, the stringent security requirements of the complex 5G architecture are not always simple to be addressed by LPWAN solutions, given their communication constraints. Even so, many research proposals from the academia are filling this gap and the secure integration of LPWAN technologies within the 5G architecture is now getting a great and firm momentum.

[1]https://www.scopus.com

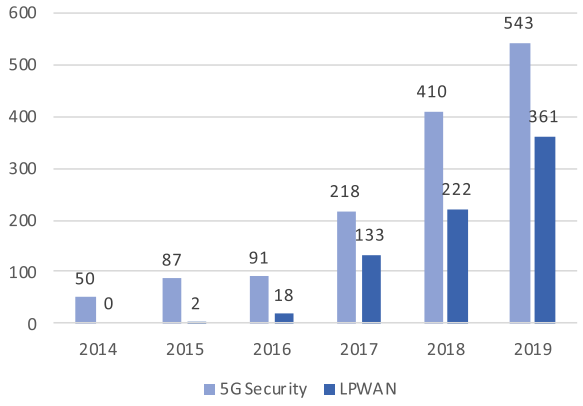

FIGURE 1. Number of "5G Security" and "LPWAN" publications indexed in Scopus during 2014–2019.

A. CONTRIBUTIONS

Unlike previous surveys that can be found in the literature [1], [2], [6]–[14], this work aims to focus on current research proposals and standardization efforts related to security aspects, mostly related to network access, which is the basis for establishing a secure communication with the network, in relevant LPWAN technologies such as Narrowband-IoT (NB-IoT) [15]–[19], LoRaWAN [20], or Sigfox [21]. These tasks are of prominent importance when deploying massive or ultra-dense networks for ensuring the overall security of the IoT architecture. We provide several classification aspects to analyze different approaches, and describe recent research papers addressing such issues. Besides, we explore the security requirements of present and future IoT applications, identifying current challenges that need to be addressed for a secure and scalable integration of LPWAN technologies within 5G infrastructures.

Table 1 summarises a comparison of related survey papers addressing similar topics as those presented in this work. Concretely, the main contributions of our work are the following: (i) a technical description addressing the security integration of 3GPP NB-IoT technology into the 5G ecosystem, (ii) a similar discussion regarding other non-3GPP IoT LPWAN technologies such as LoRaWAN, Sigfox, etc., (iii) a requirement analysis for IoT technologies in order to be integrated within the 5G architecture and support its services, (iv) an analysis of IoT use-case security requirements, (v) a comprehensive review of recent LPWAN security-related research, (vi) a discussion of international initiatives, specially focused on European efforts related to the deployment of a secure 5G ecosystem, and (vii) a review of related standardisation efforts. As can be seen in Table 1, previous survey works [1], [2], [6]–[14] do not fully cover all the aspects pointed above.

The rest of this paper is organized as follows. Section II justifies the integration of LPWAN and 5G ecosystems by

identifying key IoT-5G fields of application. The requirements of the 5G architecture for a secure integration of IoT systems are deeply discussed in Section III. A wide review of 5G-LPWAN security proposals from the academia is presented in Section IV. Open issues and research challenges in different related aspects are described in Section V. Section VI explores future research directions and trends. The paper is concluded in Section VII presenting the most important facts.

II. IoT APPLICATIONS IN THE 5G ARCHITECTURE

Many vertical industries will benefit from the generalized deployment of IoT networks and their integration within 5G architectures [1]. Smart cities [22] is one of the most studied scenarios, envisioning secure and reliable IoT connectivity [23] for novel smart applications such as energy-efficient buildings, parking control, waste management, etc. This will entail the coexistence of different type of Radios Access Technologies (RATs), from broadband connections, e.g., 4G/5G, WiFi, etc., to low-power alternatives such as Zigbee [24], 6LoWPAN [25], or LPWAN-based solutions. This opens real issues from the security perspective in order to provide a seamless connectivity to the EDs. In this line, novel authentication mechanisms should be developed for enabling a fast transition from one RAT to another one, specially in the case of using constrained communication channels such as those employed by low-power IoT devices. Another vertical that will be highly challenging to manage due to the mobility conditions of the users and EDs is Intelligent Transportation Systems (ITS) [26]. Many services have been defined under this umbrella: vehicle monitoring, goods tracking, safety applications, etc. Depending on the areas in which the vehicle is travelling, the available RATs are highly changing. In urban scenarios it is very likely to have a number of available connections, however in rural regions, only long-range technologies, e.g., LPWAN, will provide IoT connectivity. In addition, the network requirements of the different vehicular services are diverse in terms of latency, bandwidth, or reliability. Therefore, adaptive applications are needed to adjust their functioning to the available network-resources. A use case that may be integrated within these verticals (smart-cities and ITS) is eHealth [27]. Big static infrastructures such as hospitals and mobile elements such as monitored individuals or ambulances will cooperate to provide constant and real-time information about patients. This specific use case will present additional security requirements due to the highly sensitive data flowing through the network. Data leaking must be avoided while patient' identity-privacy have to be guaranteed as well. Therefore, highly secured authentication methods should be implemented in monitoring devices to ensure the source of the information and protect user's privacy.

Besides the verticals industries discussed above, which include mobile scenarios, other use cases present additional challenges in static deployments due to the lack of broadband connectivity. This situation happens when the EDs are installed in remote areas, for example in use cases of smart-grid [28] and smart-agriculture [29]. In both of them, the elements to be monitored, e.g., electric grids, or crop plantations, among others, cover wide extensions far from urban areas. Under these conditions, it is difficult and expensive to provide broadband connectivity to EDs. Therefore other communication solutions have been developed such as LPWAN technologies to cover this gap given the relevant characteristics mentioned previously [6]. For applications in rural areas, LPWAN technologies are the main solutions to provide an adequate connectivity to low-power EDs.

Different LPWAN-based solutions are being currently considered to be integrated within the 5G ecosystem. Two different families maybe identified: (i) cellular-based solutions, e.g., NB-IoT, and (ii) standalone infrastructures, e.g., LoRaWAN, Sigfox, etc. Both of them provide key features to permit low-cost and low-power IoT deployments, but their integration with 5G infrastructures presents different security issues. Regarding the first group, the security demands of 5G are considered by design. NB-IoT devices implements the 4G stack, which includes secure authentication processes as regular cellular terminals. Therefore, the NB-IoT integration in the 5G ecosystem is straightforward. On the other hand, non-cellular solutions should adapt their authentication mechanisms to be compliant with the security requirements of 5G systems. However, LPWAN solutions such as LoRaWAN or Sigfox present inherent limitations for supporting classic authentication protocols (e.g. Internet Key Exchange (IKE) or Transport Layer Security (TLS)), which opens a dangerous way of intrusion from the edge nodes towards the network core. In first place, LPWAN-based technologies are highly restricted considering the number of messages allowed for transmissions per day and their length. For that reason, considering typical authentication protocols employed in non-restricted systems is not a valid approach for these systems, as they make use of several big-sized messages. Besides, IoT EDs are usually severely limited in terms of computation capacity due to their energetic restrictions, so performing complex cryptographic operations is not a valid option to be considered. Therefore, the authentication methods under these conditions should be lightweight techniques not involving excessive communication overhead but providing the security levels demanded by 5G architectures without the need of performing heavy computations in EDs. In the following section, a comprehensive description of the requirements posed by 5G architectures in order to permit the integration of IoT networks is given.

III. 5G SECURITY FOR IoT INTEGRATION

As stated above, the network access security domain is one of the most critical aspects in 3rd Generation Partnership Project (3GPP) architectures as it covers the set of specifications and features that enable EDs to authenticate and securely access the network. From an architecture-centric perspective, these mechanisms protect the whole system from unauthorized access or attacks originated in the radio segment, so it

acts as a first and crucial defensive barrier. While off-the-self 3GPP communication technologies are compliant with standard network registration and authentication procedures defined for cellular architectures, the integration of other non-3GPP solutions like LPWAN, specially in the IoT field, is not yet clear, given the stringent security requirements posed by cellular architectures and the limited resources of many IoT devices. In the following, we explore the authentication mechanisms defined for 5G in order to understand the requirements for a potential integration of IoT solutions within these 3GPP architectures.

A. 5G SECURITY ARCHITECTURE

5G security requirements drive the need for advanced features that improve the network authentication and key management procedures with respect to previous 3GPP-defined architectures. Some of these features include a unified framework that supports different use cases, ED identity protection, and secure key derivation and distribution, among others [11]. Thus, authentication and key management are fundamental parts of the cellular network design and their secure operation in order to enable mutual authentication between end-user and the Serving Network. Also, the need for a more modular system architecture leads to the necessity of deriving crypto keys for protecting both user-plane data and radio signaling. 5G architecture has evolved from previous cellular systems by including new blocks that enrich its functionality. In this line, the 3GPP defines a set of network functions that take part in the authentication and authorization procedures. The entities that participate in this process are represented in Fig. 2 and described as follows:

- The SEcurity Anchor Function **(SEAF)** is located in the Serving Network, relying the authentication messages between the ED and the Home Network during authentication. Although this entity can either accept or reject the ED's authentication attempt, normally it follows the Home Network decision.

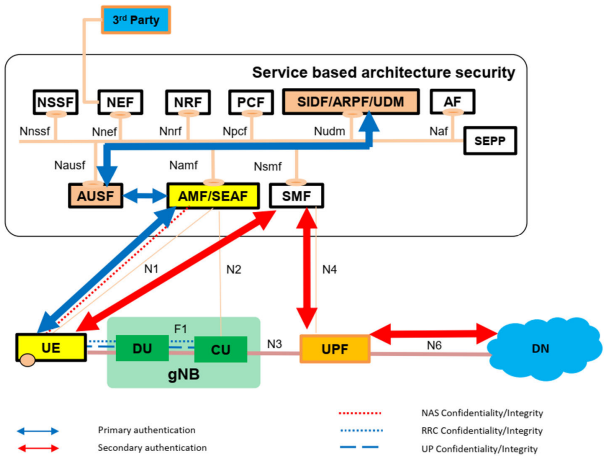

FIGURE 2. 5G Security Functions (extracted from [31]).

- The AUthentication Server Function **(AUSF)** is placed in the Home Network and accessed by the SEAF. This entity is in charge of performing direct authentication with the ED, thus deciding whether to accept or not. Also it depends on the back-end to derive session keys whenever the procedure employs 5G-defined authentication methods. Besides, it handles queries received from both 3GPP and non-3GPP access networks.
- The Authentication Credential Repository and Processing Function **(ARPF)** works within the Unified Data Management **(UDM)**, which hosts a set of functions in charge of data management. ARPF chooses the authentication method based on subscriber ID and configured policies. Additionally, it computes the session crypto material from the long-term key employed in authentication and security association purposes.
- The Subscription Identifier De-concealing Function **(SIDF)** is also found within the UDM, and provides the de-concealment of the encrypted subscriber identifier. During 5G authentication processes, the long-term identifier (i.e. the Subscription Permanent Identifier (SUPI)) is always encrypted before being transmitted over the radio link. When encrypted, the long-term identifier is known as Subscription Concealed Identifier (SUCI). More specifically, a public-key infrastructure is employed in the process, where the SIDF holds the private keys needed for decryption of the SUCI.
- The Non-3GPP Interworking Function **(N3IWF)** is needed only when the authentication is performed over an untrusted non-3GPP access network. It acts as a Virtual Private Network (VPN) server and establishes an IPSec [30] channel with the User Equipment (UE). This way, the UE may perform a secure authentication to access the core services.

All the aforementioned elements compose the 5G Unified Authentication Framework, whose goal is two-fold, namely, to make 5G authentication open by supporting standardised methods, and being access-network agnostic, i.e., working with both 3GPP and non-3GPP access networks, e.g., WiFi or fibre.

In 5G architectures, authentication and key management procedures are differentiated in *primary authentication* and *secondary authentication*. On the one hand, primary authentication defines the mechanisms that permit UEs accessing to the Serving Network domain. Hence, it is exclusively managed by mobile network operators. Additionally, in a roaming scenario, the Serving Network co-operates with the subscriber's Home Network to allow network registration and access. On the other hand, secondary authentication procedures define how to access Data Networks (DNs) outside of the cellular infrastructure itself as DNs may belong to external domains and are not necessarily managed by the telecom operator. This division is one of the new integration features of the 5G system with regards to 4G, where this distinction was not available.

1) PRIMARY AUTHENTICATION

When a UE tries to register at a specific serving network for the first time, it creates a new *5G Security Context* [32]. The data stored in this context will change through the authentication and key derivation exchanges needed by the 5G system. Additionally, the main goal of holding this information is to save resources by avoiding repeated transactions procedures, and further optimising mobility and handover processes. A UE may hold several different security contexts, one for each serving network connection. For instance, if a UE has previously accessed a serving network and both the UE and the network domain kept a copy of the security context, the serving network may re-activate the previously obtained context and skip the authentication and key derivation procedures. Besides, mobility and handover leverage on two kinds of UE registrations, namely, (i) with different serving networks, or (ii) with the same serving network but through different radio access networks. In the first case, the UE must separately authenticate with each serving network and keep one 5G security context for each operator. In the latter, the UE can access the same serving network through different access technologies, 3GPP and non-3GPP, reusing the same 5G security context even when switching access networks [32].

The 5G security context is the established local state at the UE and the serving network domain. It is composed by the 5G Non-Access Stratum (NAS) security context, the 5G Access Stratum (AS) security context for 3GPP access, and/or the 5G AS security context for non-3GPP Access. The security contexts hold different types of data like derived keys, cryptographic material, different counter variables for security algorithms, UE security capabilities, key set identifiers, etc.

In order to register at a serving network, the system must employ the two major authentication services defined by 5G, namely: (i) $N_{AUSF}UEAuthentication$ exposed by the AUSF, and (ii) $N_{UDM}UEAuthentication$ exposed by the UDM. Regarding authentication methods, 5G specifies three of them to be taken as default mechanisms, namely: (i) 5G-AKA [32], (ii) Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') [33], and (iii) the EAP-TLS Authentication Protocol (EAP-TLS) [34]. These authentication and key exchange methodologies are described in the following:

(i) 5G-AKA: Fig. 3 showcases the sequence diagram of the 5G-AKA exchange. As a common procedure to all the authentication methods mentioned above, first, the UE sends a registration request including its SUCI to the SEAF in order to start the authentication process. Next, the SEAF begins the authentication process with the Home Network by sending an authentication request to the AUSF. This permits the AUSF to verify if the Serving Network is authorised to perform such task. In turn, the AUSF will send the authentication request to the UDM/ARPF. Since the SUCI is provided, the SIDF will be invoked to obtain the long-term identifier in its plain-text form, i.e., the SUPI. Finally, the SUPI is employed by the system to choose the authentication method and policies regarding the UE.

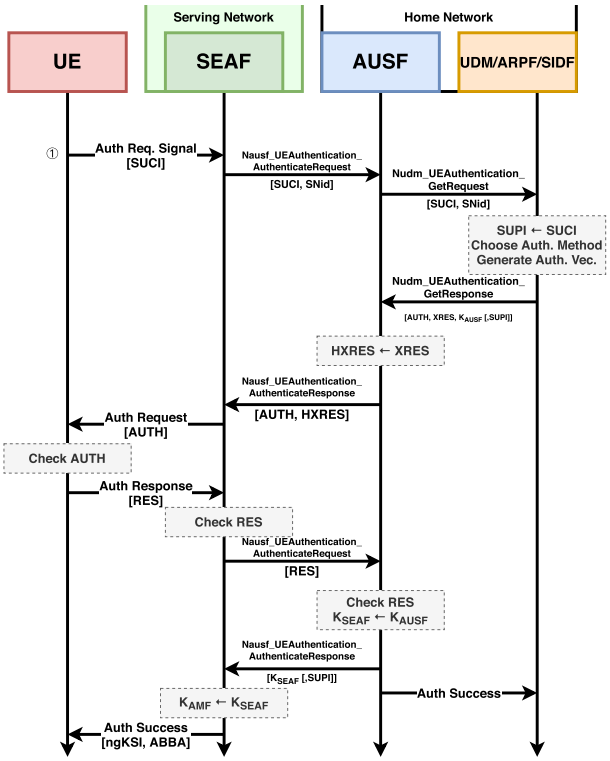

FIGURE 3. 5G-AKA exchange sequence diagram.

Then, the UDM/ARPF starts its specific procedure by sending an authentication vector that contains the authentication token, *AUTH token*, the expected response token, *XRES token*, and the authentication and encryption derivation key, K_{AUSF}. Optionally, if the SUCI was included in the request, the SUPI is added to the preceding fields as follows: $[AUTH, XRES, K_{AUSF}, [SUPI]]$.

Next, the AUSF stores the K_{AUSF} and computes the hash of the expected response token as *HXRES*, which in turn is bundled with the *AUTH token* and sent together to the SEAF as [*AUTH token*, *HXRES*]. Next, the SEAF stores the *HXRES* and sends the *AUTH token* to the UE. In turn, the UE validates the received *AUTH token* with the shared key, which is only known by the Home Network. At this point, if the validation was successful, the UE considers the network as authenticated. This ends the first stage of the procedure; as a result, the UE has derived its local copy of the key hierarchy. The UE will follow by notifying the Serving Network of the successful result of the operation.

Then, the UE sends the authentication response message in order to continue the process by generating the authentication response token, *RES token*, and sending it to the SEAF. The SEAF validates the *RES token* and delivers its contents to the AUSF. As mentioned above, the AUSF in the Home Network ultimately decides if the authentication is accepted or rejected. If the AUSF accepts the *RES token* as valid, it generates the anchor key, K_{SEAF}, and sends it back to the SEAF. Optionally, if the SUCI was included in the original

registration request, the SUPI is added to the response. As soon as the SEAF receives the K_{SEAF}, it derives a K_{AMF} and deletes the K_{SEAF}. Then, it will notify the authentication's success to the UE, including other security parameters that allow the UE to derive the K_{AMF} locally. The Access and Mobility Management Function (AMF) will employ K_{AMF} to generate the confidentiality and integrity keys that protect UE's signaling. Finally, the AUSF notifies the UDM/ARPF about the result of the procedure for logging and auditing purposes. As aforementioned, the UE keeps hold of the long-term key that is employed to derive all the key hierarchy. Hence, the UE will share a local copy of the whole set of keys. Note the important function of the K_{SEAF}, known as *anchor key* in 5G-AKA procedures, employed in both 3GPP and non-3GPP access networks aiming at identifying an authorised Serving Network, thus preventing Serving Network impersonation attacks.

(ii) EAP-AKA' in 5G: If either EAP-AKA' or EAP-TLS are employed instead of 5G-AKA, then the UE and AUSF act as EAP end-points [35]. In this scenario, the UE and AUSF behave as EAP peer and server, respectively, and the SEAF plays a pass-through role during the authentication process. Like 5G-AKA, EAP-AKA' is based in the challenge - response principle, with a shared secret key known by both UE and Home Network. Likewise, it obtains the same security features as 5G-AKA. However, the message exchange is different to those of 5G-AKA as shown in Fig. 4.

First, similar to the 5G-AKA method, the UE launches the primary authentication process by sending a registration request signal that will eventually reach the UDM. With the data contained in the registration request, the UDM attains the UE's SUPI and the authentication method is chosen based on the user policies. Then, a regular EAP-AKA' exchange takes place as described in RFC 5448 [33]. During this procedure, EAP payloads get encapsulated in NAS packets when travelling between UE and SEAF. Then, they are forwarded within 5G service messages from SEAF to the AUSF. As aforementioned, in EAP-AKA' the SEAF forwards certain messages without taking part in the authentication decision process.

(iii) EAP-TLS in 5G: EAP-TLS is mainly defined in 5G to be used in specific deployment modes of operation. The most typical scenarios are private networks or IoT environments. The architecture is similar to that of EAP-AKA', i.e., the authentication end-points are the UE and AUSF, with the SEAF assuming the role of transparent forwarder. Nevertheless, EAP-TLS presents fundamental differences with the other authentication methodologies. Its main characteristic is the trust model established between the UE and network. EAP-TLS mutual authentication between them leverages on trust of public certificates. In some cases pre-shared keys (PSKs) can also be employed. However, in AKA-based methods, the trust exclusively leverages on the shared symmetric key pre-installed in both UE and network. EAP-TLS removes the need of managing and storing large amounts of long-term keys at the Home Network. This considerably

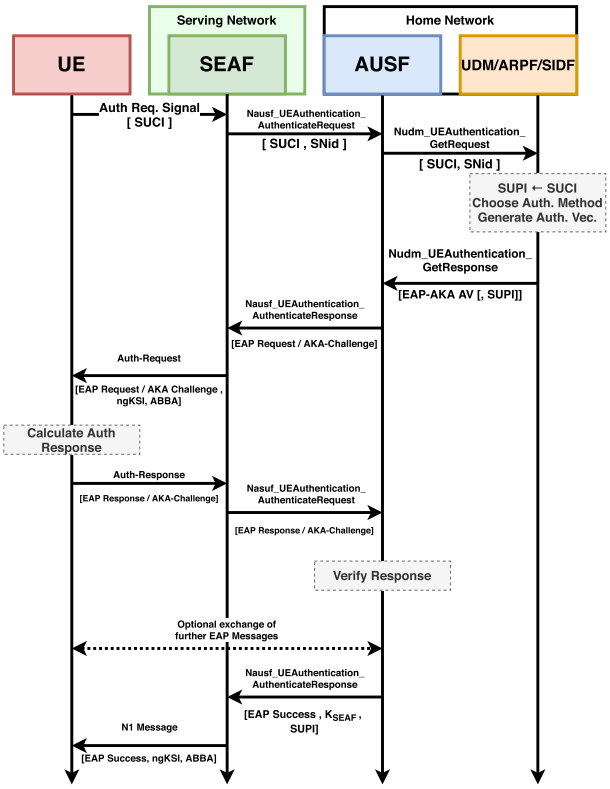

FIGURE 4. Authentication procedure for EAP-AKA'.

reduces key management issues, at the cost of introducing a Public Key Infrastructure (PKI) into the system.

In order to obtain mutual authentication, both the UE and AUSF can verify each other's certificates or PSKs. Both of them must have been previously established either in a previous TLS handshake or by means of out-of-band methods. At the end of the EAP-TLS process, an Extended Master Session Key (EMSK) is derived and the K_{AUSF} is taken from the lowest 256 bits of it.

Fig. 5 presents the 5G EAP-TLS protocol steps. Given their complexity, in the following we provide a comprehensive description of these steps.

1) Similar to the rest of primary authentication methods, first, the UE sends a registration request signal to the SEAF in the Serving Network. As aforementioned, this registration request includes the UE's SUCI. Upon receiving this message, the Serving Network starts the authentication process by including its identifier and forwarding this message to the Home Network. The AUSF checks that the identifier belongs to a legitimate Serving Network and, in that case, the request gets passed onto the UDM to obtain the SUPI by deciphering the SUCI.

2) The UDM checks the policies associated to the received SUPI, this way, the authentication method to be used is determined. Thereby, it signals the AUSF that 5G EAP-TLS is the chosen authentication method. In turn, the AUSF sends a *TLS_START* to the UE through the SEAF, indicating the UE that the EAP-TLS procedure has been initiated.

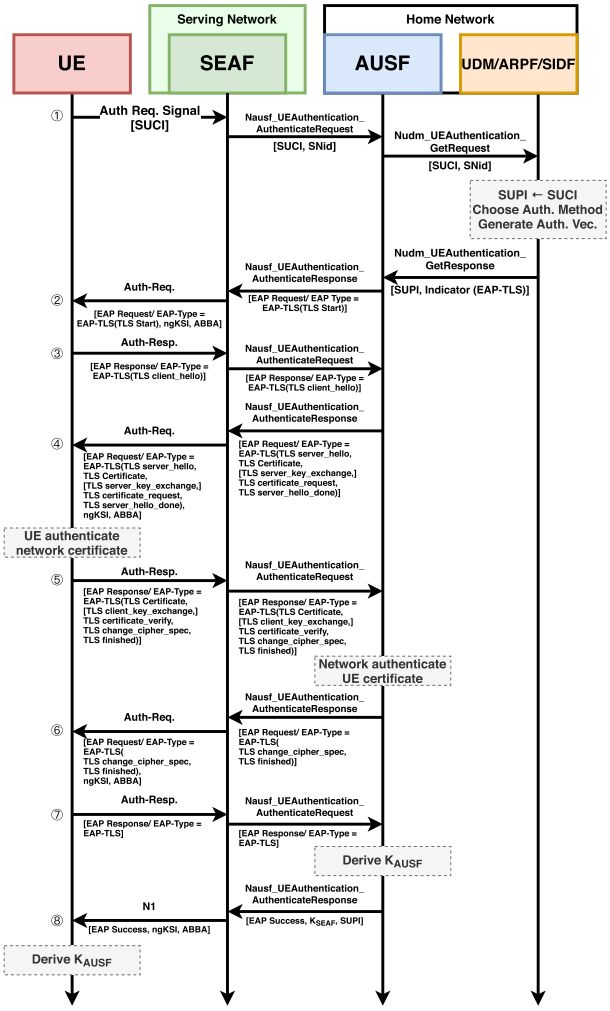

FIGURE 5. EAP-TLS authentication procedure over 5G networks for initial authentication.

3) The UE aggregates several ciphering attributes that include a list with the supported algorithms by the UE. This message is known in the EAP-TLS exchange as the *client_hello*.

4) The AUSF answers the UE with its own ciphering attributes, including the supported algorithms, and the Home Network certificate. This EAP message is known as *server_hello*. Note that as EAP-TLS supports several TLS versions, negotiating the version to be employed is part of the *client_hello/server_hello* exchange. The protocol procedure described here follows the RFC5216 [34] standard, which uses TLS v1.1. Finally, the UE validates the Home Network by verifying the received certificate. If the check successes, at this point in the procedure, the UE considers the Home Network as authenticated. As aforementioned, the UE is able to validate the certificate because a previous trust model is established.

5) Next, the UE generates a session key $K_{session}$ as detailed in [34], which will be employed during the rest of the exchange. Likewise, it computes several crypto attributes including a hash of the previous handshake messages, i.e., steps 2, 3, and 4. They are added to the following package that also includes a copy of the UE's certificate. Additionally, the *change_cipher_spec* signals the other end-point a success in the algorithm negotiation, indicating that the chosen algorithm will be employed during the rest of the handshake. When receiving this message, the AUSF verifies the UE's certificate, hence the Home Network considering the UE as authenticated. Similarly to the UE, the Home Network is expected to be pre-configured with all the material needed to validate the UE's certificate. Alternatively the Home Network may use the PKI to attain such information. Then, the AUSF also computes the hash of the previous handshake messages and checks if the values match with those received from the UE. As a result of these computations, the AUSF derives the session key $K_{session}$.

6) The AUSF encrypts its computed hash of the previous handshake messages, i.e., steps 2-4, with the $K_{session}$, and sends it to the UE. Upon reception, the UE will check if the received hash equals its own copy. If they match, the UE considers the authentication process successful.

7) To indicate the end of the procedure, the UE sends an *EAP_TLS* message to the SEAF, which forwards it to the AUSF. The AUSF generates a new K_{SEAF} using crypto attributes exchanged during the handshake.

8) Finally, the AUSF sends the K_{SEAF} and the SUPI together in a success message to the SEAF. The SEAF forwards the success message to the UE. Then, the SEAF considers the primary authentication process as completed. In turn, the UE derives its own copy of the K_{SEAF}. From this point onward, all the communications will be encrypted with the K_{SEAF}.

There are two 5G security parameters employed in all primary authentication methods described above, namely the 5G Key Set Identifier (ngKSI) and the 5G Anti-Bidding down Between Architectures (ABBA) parameter. Both of them are sent from the SEAF to the UE, in order to securely derive the K_{AMF}. On the one hand, the ngKSI parameter is an identifier that points to the specific key set in the partial security context employed during the key exchange procedure. On the other hand, the ABBA is a parameter meant to provide flexibility and security in future 5G releases. It is initialised to zero and updated each time the security parameters are changed during authentication. This way, the system avoids attacks related to one party switching to a lower security release midway.

As a result of a UE authentication process, a number of implications take place, namely:

- The Serving Network must authenticate the UE with its identifier in plain-text, i.e., the SUPI.
- The UE also authenticates the Serving Network as a side effect of the authentication and key agreement process.
- The Serving Network gets authorization by the Home Network to provide access and services to the UE.
- The UE will get assurance that it is connected to an authorized *Access Network*.

- The Serving Network will authorize the UE's access to the offered services based on its profile.
- *Unauthenticated Emergency Services* will be granted to UEs in order to meet the region regulations.

2) NON-3GPP ACCESS TECHNOLOGIES

As explained before, the underlying aim of 5G authentication procedures is to support several kinds of accesses by exploiting a series of standardised mechanisms [36]. To enable that, the core provides each UE with specific interfaces for user and control planes. These are employed to communicate with the device, regardless of the employed access technology.

To keep the unified association between UE and Serving Network despite the network access methodology, there are some common protocols and services kept in both 3GPP and non-3GPP access. Some of the most relevant services include the same NAS protocol between the UE and 5G core, through the so-called *N1 interface*. Also, the same User Plane Function (UPF) service maintains the Packet Data Unit (PDU) session despite the UE switching from and to 3GPP or non-3GPP technologies. This improves the overall efficiency of advanced mobility services because only one UPF is involved in 3GPP and non-3GPP access. Nevertheless, some particular aspects of 3GPP standardised technologies are lost when the non-3GPP access is employed. For example, the User Location Info (ULI) service providing geographical position data employs the cell identifier that the UE employs to access the core. However, there is no such functionality defined when the UE employs non-3GPP access. Another feature not available for non-3GPP accessing UEs is the Discontinuous Reception (DRX) procedure that notifies the existence of downlink information waiting to be transmitted. Lastly, the handover processes of 3GPP technologies is managed by the Radio Access Network (RAN); in contrast, non-3GPP EDs manage the handover themselves without external support.

Since there is only a single control plane connection for each UE, this allows the 5G core to manage the device in a similar manner, despite employing 3GPP or non-3GPP access technologies [37]. This is possible thanks to common services like the NAS signaling, address allocation, or policy enforcement. As a result, the management effort is coordinated by converging all the traffic to the same core. Traffic flows from the core or originated in the access network may be efficiently optimised in an end-to-end basis. Thanks to this design, the UPF retains an overall vision of all anchored accesses, from and to the UE. At the same time, the AMF has the visibility over all radio links statuses and the radio spectrum availability. All the aforementioned design choices enable high performance features like load balancing, more accurate access technology selection, core network traffic optimisation, and end-user energy performance, among others.

In 5G, UE access to the Serving Network through non-3GPP technologies is established by a signaling between the UE and the core. First, the UE connects to the chosen non-3GPP access network by procedures outside of 3GPP specification scope, e.g., WiFi. This connection may or may not be secured, with regards to data confidentiality or integrity. From the viewpoint of the 5G, it does not matter because the 5G core does not rely on the non-3GPP technology's security features. Thus, the UE starts communicating with the N3IWF employing the non-3GPP access technology as a mere carrier of signaling information. The end-goal of this procedure is to establish a secure signaling connectivity between UE and the serving network over an untrusted channel, namely, the non-3GPP access network. In order to achieve this, an IPSec link is attained between UE and AMF. The UE receives the N3IWF's IP address from the access network and begins an IKE [38] exchange with the N3IWF. The goal is to protect both UE and N3IWF from possibles attacks over the untrusted non-3GPP access network. The IKE procedure complies with the RFC7296 specification with a few adjustments, i.e., the UE will provide the N3IWF with its AMF identifier so that it can negotiate access to the core. Through the AMF, the UE establishes its NAS signaling channel with the 5G core, employed in further services like registration or authentication signaling. Note that, at this point the IKE exchange is still halfway its authentication phase, hence using the EAP-5G protocol, the NAS signaling is sent as a specific variation of the common EAP defined in RFC3748 [35]. Finally, the AMF provides the N3IWF with security material needed to finish the IKE establishment. Moreover, an IPSec security association is achieved, dedicated to NAS signaling. From that moment, the NAS signaling travels embedded within the IPSec tunnel.

3) SECONDARY AUTHENTICATION

As mentioned previously, secondary authentication procedures define how to access data networks (public or private) outside of the cellular infrastructure itself. One of the advantages of secondary authentication is that devices can access the data network regardless of their communication technology. It employs standardised EAP technologies through the Serving Network to transparently access the target domain without specific customization by the administrators, thus improving flexibility of deployments by broadening the type of compatible devices. This is specially relevant in IoT scenarios due to the heterogeneity of devices composing them. Secondary authentication is optional and, as a pre-condition, the UE must be registered in the Serving Network and have a network access security context, obtained through primary authentication.

In this scenario, UE, Session Management Function (SMF), and external Authentication, Authorization and Accounting (AAA) [39] server act as the EAP peer, authenticator, and server, respectively. The authentication procedure is started by the UE, which sends a PDU session establishment request to the Serving Network. This request contains all the authentication and authorisation information required for the Serving Network to identify the specified Data-Network Authentication, Authorisation, and Accounting (DN-AAA) server. Next the AMF, SMF, and UPF within

the Serving Network forward the EAP request/response messages between UE and DN-AAA. All authentication and key derivation messages pass through the Serving Network. Finally, after a successful EAP authentication, the DN-AAA sends an *EAP-Success* message to the SMF, which stores the new security relationship between UE identifier and data network identifier (DNN). This ends the secondary authentication procedure and gives way to a new PDU session establishment procedure initiated by the UE.

B. REQUIREMENTS FOR SECURE IoT APPLICATIONS OVER 5G

Being able to cope with a highly dynamic ecosystem is one of the 5G security drivers [36]. Current cellular networks are dominated by monolithic deployments controlled by a single network operator which owns all the radio access and system infrastructure, and manages all the offered services. In turn, 5G is aimed at supporting several specialised stakeholders that will provide end-user network services. For this reason, 5G security requires high flexibility in order to efficiently support any unexpected use-case or application. For instance, security mechanisms devoted to ultra-low latency mission-critical communications may not be adequate for massive IoT deployments consisting of constrained devices sporadically sending small packets.

5G service requirements are collected in [40]. These were identified by 3GPP's service and system technical specification group (TSG-SA) and include the security requirements of IoT applications. The IoT umbrella covers EDs with different characteristics, e.g., diverse life-cycles, long life-spans of years, lack of keypads or displays, etc. These devices may change owner several times, e.g., inherited IoT deployments or consumer goods, and, in many cases, there are not any solution for customization or firmware modification. Additionally, the majority of these devices can operate autonomously without human supervision. This drives the need to dynamically establish or refresh cryptographic material such as credentials. Although there are some out-of-band (OOB) bootstrapping protocols currently under standardisation [41]–[43], they require physical access for each device to be updated, which greatly increments management overhead.

IoT devices are not only heterogeneous in their computing power but also in their networking capabilities. Different-purpose EDs may require the transmission of packets with diverse lengths employing different communication channels and using a variety of data-rates; for example, periodic report packets from a light post may not be as urgent as the alarms triggered by a fire detector. Moreover, some IoT scenarios would prefer fairness in network resource allocation, i.e., all devices have similar available network resources for transmitting/receiving data. In this line, 5G security is also characterized by the need of seamlessly available access-independent security mechanisms due to the constant emergence of novel access technologies, including licensed and unlicensed, 3GPP and non-3GPP.

In order to handle the discussed security requirements, and as described in the previous section, 5G manages authentication employing a unified framework. Some of its main security requirements include support of efficient authentication means for a wide range of IoT devices, and the use of a suitable authentication framework, namely EAP, to allow alternative authentication mechanisms to those standardised by 3GPP, e.g., 5G-AKA. These mechanisms may employ different types of credentials defined by standardisation bodies outside of the 3GPP when accessing non-public networks [40]. Besides, the 5G authentication shall also support alternative authentication methods defined by the operator with different types of credentials for IoT deployments in private and isolated deployments.

The lack of trust in a roaming partner is another major 5G security design choice [44]. As Home Networks do not usually trust the Serving Networks employed by EDs, the full control of authentication and key derivation processes is given to the former. Through these procedures, the Home Network is able to discover if the ED is connected to the legitimate Serving Network, and not a malicious impostor. 5G standardisation has chosen EAP as a suitable authentication framework because it is compatible with different methods that can match the specific use-case characteristics and needs. With a focus on flexibility and scalability, EAP and AAA are key technologies in massive IoT use case integration [45].

Finally, bandwidth efficiency is one of the major concerns regarding massive IoT scenarios. 5G security requisites [40] indicate that the system shall minimize the security signalling overhead without compromising the level of system protection. With the arrival of LPWANs, the IoT long-range and energy efficient networking gap has been partially filled. However, these notable characteristics are attained through the severe expense of having a highly constrained communication channel. In general, LPWANs were designed with support for a few packets each day per device. This limitation is even more exacerbated in unlicensed LPWAN technologies like LoRaWAN or Sigfox. As a result, confidentiality and privacy schemes exchanging packets larger than tens or hundred bytes are prohibitive. For this reason, authentication and privacy protocols for non-constrained scenarios are not commonly used in constrained IoT. Therefore, in massive IoT there is a preference for reduced protocol layers, due to the implicit overhead of having more headers [46]. Another reason to prefer shorter packets is to avoid fragmentation; for example, typical long security messages including cryptographic material would need to be fragmented for being used in LPWAN networks. This can potentially open new attacks vectors that exploit reassembly state and exhaustion [46]. Section V reviews additional challenges regarding the integration of IoT and 5G.

C. 5G IDENTITY MANAGEMENT

The 5G architecture should protect the subscriber identity together with other user's sensitive data from both passive and active attacks [40]. This goal has been addressed since

the beginning of the standardisation process as described as follows. The *5G Phase 1* [44] introduced several main security enhancements related with user and data privacy, namely, (i) user privacy through the protection of the long-term permanent identifier, and (ii) user plane integrity protection. Each (U)SIM card contains a fixed long-time identifier attached to the subscription. This was commonly known in 4G as International Mobile Subscriber Identity (IMSI), renamed as SUPI for 5G systems. Since 5G primary authentication is based on a pre-shared trust relationship, first, it is needed to identify the user while the connection establishment. However, sending the plain-text long-term subscriber identifier over radio may result in the user being identified, located, or tracked. 4G-LTE systems avoided sending the plain-text IMSI by employing a temporary identifier instead, namely, the Temporary Mobile Subscriber Identity (TMSI). This temporary identifier is assigned by the visited network, mapping to the long-term identifier at the core. Likewise, 5G employs the analogous 5G Global Unique Temporary Identifier (5G-GUTI) that fulfills the same role.

However, in legacy 4G systems, there are situations when the UE needs to send the IMSI in plain-text instead of the TMSI. For instance, when the ED registers for the first time in a visited network or if the core network itself cannot resolve the mapping of the temporal ID to the long-term identifier. This behaviour can be exploited by attackers by employing a 4G-LTE base-station that triggers the transmission of the plain-text IMSI by the UE. This attack is known as *IMSI Catching* and has been a vestigial vulnerability of 4G-LTE systems for decades. This is because 4G retained backwards compatibility with all the previous systems, i.e., GSM and 3G. The 3GPP solution to this issue is brought by 5G in the form of the Subscription Concealed Identifier (SUCI). This design choice sacrifices backwards compatibility with previous 3GPP systems by never allowing the transmission of plain-text user identifiers over radio interfaces. The motivation of the SUCI is to protect the user identity from malicious visited networks and passive radio attacks. The SUCI is encrypted using the Home Network's public key, contained in the (U)SIM card. Thus, the long-term credentials stored in the UDM must remain secure during the ED's lifetime.

Regarding user plane integrity aspects, the protection is limited to the UE's chipset capabilities. Some offer cryptography functions limited by the transmission bit rate, for example in the user plane [44]. Although this is a valid solution for most of massive IoT use-cases given the limited traffic produced/received by each ED, this is an issue to be addressed.

IV. SECURITY SOLUTIONS FOR LPWAN-5G INTEGRATION

In recent years, the security aspects related to the LPWAN-5G integration have attracted a significant interest from the research community. This section describes the main proposals addressing security aspects of LPWAN-based technologies and their relationship with the integration into the 5G ecosystem based on the security mechanisms described in the previous section. Our analysis also covers research works that do not explicitly address the integration of LPWAN in 5G, but are focused on security aspects that can be also considered for such integration.

A. CLASSIFICATION ASPECTS

Before describing the different surveyed research proposals, we propose diverse aspects to help in the classification and analysis of the current landscape of approaches:

- *LPWAN technology*: As described in recent works [7], [47], current landscape of LPWAN solutions is still fragmented. Indeed, there is a plethora of existing technologies, including Dash7 Alliance Protocol Low-Rate (D7AP Low-Rate) [48], Weightless [49], Extended Coverage GSM (EC-GSM) [50], or LTE Cat-M1 (LTE-M) [51]. However, we focus our analysis on the technologies that are considered in the scope of the Internet Engineering Task Force (IETF) RFC 8376 [52], namely, LoRAWAN, NB-IoT, Sigfox, and Wi-SUN FAN [53]. The main purpose to consider such technologies is to narrow down our analysis to communication approaches that are contemplated under current standardisation actions.
- *Security aspects*: Most of current works are focused on a specific security aspect for the LPWAN-5G integration. According to our analysis, authentication, key management and the prevention of different security attacks represent the most widely considered concerns in existing literature. Furthermore, as already mentioned, we also include in our analysis research proposals coping with additional security aspects of LPWAN technologies, as they provide insights to be considered for the integration into the 5G ecosystem.
- *5G integration*: The third aspect to classify the different research proposals is related to its level of maturity, i.e., if the solution has been implemented and validated. As will be described in Section IV-F, some of the proposals do not address explicitly the integration within the 5G architecture or such integration is only conceptually considered.
- *Use case/Application*: While most of the research works analyzed are intended to be used in any IoT-enabled scenario, some of these proposals are focused on specific use cases or applications, such as smart agriculture [54] or industrial IoT [55]. A description of potential applications was provided in Section II.

These aspects have been used to classify the research proposals that are described in Section IV-F. Furthermore, Table 2 provides a summary of such analysis. Before this comprehensive review, in the following we provide a general overview of the main LPWAN technologies being considered in this work with an emphasis in their off-the-shelf security mechanisms.

TABLE 2. Research papers addressing security aspects in LPWAN technologies.

Research proposal	Year	LPWAN Technology	Security aspect addressed	5G integration	Implemented/ Validated	Application	Approach
Enhancing LoRAWAN security through a lightweight and authenticated key management approach [69]	2018	LoRaWAN	Key Management	No	Yes	Generic	Use of the EDHOC protocol to update the NwkSKey and AppSKey session keys
Enabling Roaming across Heterogeneous IoT Wireless Networks: LoRaWAN meets 5G [95]	2020	LoRaWAN	Authentication	Yes	Yes	Generic	Proposal of a handover roaming mechanism for LoRaWAN, enabling 5G and LoRaWAN authentication
Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things [94]	2018	LoRaWAN	Authentication, Key management	Yes	Yes	Industrial IoT	Modification of LoRaWAN gateways to use 4G/5G cryptographic material to ensure end-to-end confidentiality and integrity
A CoAP-based network access authentication service for low-power wide area networks: LO-CoAP-EAP [73]	2017	LoRaWAN	Key Management	No	Yes	Generic	Integration of CoAP-EAP and AAA infrastructures to generate the AppKey through a bootstrapping process
Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network [60]	2019	NB-IoT	Authentication	Yes	Yes	Generic	Proposal of a certificateless scheme to improve the efficiency of NB-IoT authentication
On track of Sigfox confidentiality with end-to-end encryption [108]	2018	Sigfox	Key Management	No	Yes	Generic	Comparison of different encryption techniques for confidentiality of Sigfox systems
5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks [107]	2018	NB-IoT	Traffic filtering	Yes	Yes	Generic	A mechanism for traffic filtering in NB-IoT scenarios with mobility requirements
A dual key-based activation scheme for secure LoRaWAN [65]	2017	LoRaWAN	Key Management	No	Yes	Generic	Separation of key management tasks between a network and an application server for LoRaWAN
A secure device-to-device link establishment scheme for LoRaWAN [87]	2018	LoRaWAN	Key Management	No	Yes	Generic	Improved LoRaWAN key management scheme to support device-to-device communication
A Simple and Efficient Replay Attack Prevention Scheme for LoRaWAN [86]	2018	LoRaWAN	Replay attack prevention	No	Yes	Generic	A replay attack prevention scheme for the LoRaWAN joining mechanism by following the standard packet structure
An enhanced key management scheme for LoRaWAN [82]	2018	LoRaWAN	Key Management	No	Yes	Generic	Use of the Rabiit cipher scheme to enable the updating of LoRaWAN AppKey and NwkKey keys
An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system [66]	2018	LoRaWAN	Key Management	No	Yes	Smart buildings	Enhanced LoRaWAN key management to enable end-to-end security between device and application server.
Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system [62]	2019	NB-IoT	Authentication	Yes	Yes	Generic	An efficient and quantum-resistant authentication scheme for the integration of NB-IoT devices in 5G
LoRaWAN Authentication in RADIUS [77]	2017	LoRaWAN	Authentication	No	No	Generic	Standardization proposal for the integration of LoRaWAN with RADIUS
LoRaWAN Authentication in Diameter [79]	2017	LoRaWAN	Authentication	No	No	Generic	Standardization proposal for the integration of LoRaWAN with Diameter
Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks [98]	2019	NB-IoT	Authentication	Yes	Yes	Generic	A certificateless multi-party authenticated encryption scheme for NB-IoT devices based on their serial number
A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure [89]	2019	LoRAWAN	Authentication	No	Yes	Generic	Two-factor authentication mechanism for the join procedure, in which the information of EDs is stored in Ethereum
NB-IoT for D2D-enhanced content uploading with social trustworthiness in 5G systems [104]	2017	NB-IoT	Trust management	No	Yes	Social IoT	Establishment of a NB-IoT topology based on a trust and reputation model for IoT devices
Reliable and Secure Constellation Shifting Aided Differential Radio Frequency Watermark Design for NB-IoT Systems [97]	2019	NB-IoT	Attack prevention	No	Yes	Generic	A mitigation approach for several security attacks and eavesdropping in NB-IoT based on the received signals
Research on PUF-based security enhancement of narrow-band Internet of Things [103]	2018	NB-IoT	Authentication	No	Yes	Generic	Use of PUF to enhance security of NB-IoT devices
Research on End-to-End Security Authentication Protocol of NB-IoT for Smart Grid Based on Physical Unclonable Function [102]	2019	NB-IoT	Authentication	No	Yes	Smart grid	A PUF-based mechanism for the key derivation process between NB-IoT devices and smart grid platforms
Secure Authentication and Credential Establishment in Narrowband IoT and 5Gs [100]	2020	NB-IoT	Authentication, Key management	Yes	Yes	Smart agriculture	Integration of the LO-CoAP-EAP to carry out the initial authentication (bootstrapping) of NB-IoT devices
Secure Session Key Management Scheme for Meter-Reading System Based on LoRa Technology [71]	2018	LoRAWAN	Key Management	No	Yes	Smart grid	Enhanced key management and update mechanism based on a trusted key distribution server for smart grid scenarios
Security of join procedure and its delegation in LoRaWAN v1. 1 [81]	2018	LoRAWAN	Key Management	No	No	Generic	Security analysis of the LoRaWAN 1.1 join procedure and backward compatibility
Enhancing Key Management in LoRaWAN with Permissioned Blockchain [91]	2020	LoRAWAN	Key Management	No	Yes	Generic	Use of permissioned blockchain to improve key management in LoRaWAN
Trusted third party based key management for enhancing LoRaWAN security [84]	2017	LoRAWAN	Key Management	No	Yes	Generic	Enhancement of key management in LoRaWAN by adding a trusted third party
Using blockchain technology to build trust in sharing LoRaWAN IoT [92]	2017	LoRAWAN	Key Management	No	Yes	Generic	Use of blockchain to extend network servers functionality in LoRaWAN for key management aspects
Towards automatic deployment of virtual firewalls to support secure mMTC in 5G networks [106]	2019	NB-IoT	Attack prevention	Yes	Yes	Generic	Deployment of virtual firewalls to protect NB-IoT traffic based on SDN and NFV concepts
Secure decentralised deployment of LoRaWAN sensors [85]	2020	LoRaWAN	Key Management	No	Yes	Generic	Re-keying approach based on the use of a smartphone to transfer the device's credentials

B. LoRaWAN

LoRaWAN is one of the solutions based on LPWAN that has received more attention from academia and industry in recent years. This technology is supported by large companies such as Cisco or Semtech, which have joined together through the LoRa Alliance.[2] LoRaWAN provides a well-defined two-layer architecture: the lowest layer LoRa defines the physical (PHY) level, and above this layer, the medium access control (MAC) level is defined by LoRaWAN. The technology uses unlicensed frequency bands, so it has been widely adopted.

The LoRaWAN architecture consists of a set of EDs that are enabled to communicate with multiple gateways using a star topology. Then, a *network server* receives the messages from the end-nodes through the gateways. To participate in a LoRAWAN network, each device must be *activated* by following the Over-the-Air Activation (OTA) or Activation by Personalization (ABP) procedures. In the first case, the device and the network server carry out a joining process by using an AES-128 shared key (AppKey), which is used to derive two symmetric keys: a network session key (NwkSKey) and an application session key (AppSKey). While the NwkSKey is used between the device and the network server, the AppSKey is used to encrypt/decrypt the message payload between the device and an application server. On the other hand, in the case of ABP it is assumed that EDs are already equipped with both keys. Such keys are used to provide basic security aspects, including integrity checking and device authentication.

It should be noted that the previous description is based on the LoRAWAN 1.0 specification [56]. However, as reported by different works that are reviewed in section IV-F, this simple security approach implies different issues, especially regarding key management aspects. In order to mitigate some

[2]https://lora-alliance.org/

of these problems, the LoRaWAN 1.1 specification [57] considers two keys (AppKey and NwkKey) that are used to derive different session keys. This way, key management aspects are separated for network and application data. Additionally, this version of LoRAWAN improves authentication and key management by providing a re-join mechanism, which can be used for handover between two networks, key refreshing or even to change the ED's address

C. NARROWBAND IoT (NB-IoT)

NB-IoT was specified in 3GPP's release 13 [58], and it is characterized by enabling low cost terminals, long battery life and massive capacity [59]. This LPWAN technology is integrated into the Long Term Evolution (LTE) standard, so that it can be activated in the existing LTE networks with a software upgrade in the operator's base stations [52]. NB-IoT provides three different operation modes. In the *in-band* mode, the narrowband is deployed within a LTE carrier. In the *guardband* mode, NB-IoT can use the unused resources by LTE. In the case of the *standalone* mode, the narrowband is deployed in a dedicated spectrum.

As described in [60], the NB-IoT architecture is based on an enhanced version of the LTE-A one [61] aiming at meeting the requirements of NB-IoT devices. In particular, it includes the *control plane*, which makes use of the Service Capability Exposure Function (SCEF) to send IP and non-IP data between the NB-IoT node and the LTE-A network. The SCEF component exposes service and network capabilities in a secure way, and provides authentication mechanisms. Furthermore, the *user plane* enables the communication following the LTE approach. It should be noted that the specification of NB-IoT is linked to the 3GPP, so the integration into the 5G ecosystem is already considered. Indeed, as discussed in [62], 5G authentication mechanisms such as 5G-AKA and EAP-AKA' need to be implemented by NB-IoT devices (or UEs using the 3GPP terminology).

D. SIGFOX

Sigfox is the name of a network operator and an LPWAN technology, which was firstly launched in France in 2009. Currently, Sigfox offers their IoT solution over 30 countries in partnership with several network operators.[3] Its main purpose is to be used by highly-constrained autonomous and battery-operated IoT devices that send a limited number bytes over a specific period of time, which allows the devices to operate with a single battery for more than 10 years [21].

The Sigfox radio protocol is non connection-oriented and it is optimized for uplink communications. The capacity of a base station relies on the number of messages emitted by the devices rather than the volume of the latter. Similarly, the duration of the battery relies on the number of messages generated by the device. Sigfox makes use of the Ultra Narrow Band (UNB) transmission technology, which consists of using narrow channels of the spectrum to reach long distances, whilst reducing the energy requirement to do so. The coverage of Sigfox cells depends on the link allowance and on the location of the actual deployment, e.g, rural, urban, etc.

The Sigfox architecture is supported by a Central LPWA Gateway or a Cloud-based Service Center. In communication with Sigfox EDs there are a number of Cooperative Radio Gateways, called base stations, with support for Multiple Input Multiple Output (MIMO) communications. Regarding authentication, Sigfox uses a Central and Global Authentication system. This means that there is no need for supporting roaming. In terms of communications, Sigfox provides an unique device ID of 32 bits, supports fragmentation and asynchronous unicast communications. To secure the communications, it provides message integrity with authentication code (MAC) at link layer generated using the device ID and AES-128. Application layer encryption is optional, depending on the specific application.

In Sigfox deployments, the information is encrypted using AES-128 in counter mode with cipher keys being independent for each device. These keys are associated with the unique device ID and there are different keys for integrity and confidentiality. The key material in Sigfox is pre-provisioned, hence the bootstrapping process [46] is not considered in this technology. Lastly, Sigfox uses the pre-provisioned keys directly to perform the crypto operations, it does not derive key material from the pre-provisioned keys, which is a notable risk if the keys are compromised.

E. WI-SUN ALLIANCE FIELD AREA NETWORK (FAN)

The Wi-SUN Alliance is a global member-based and non-profit association composed of industry leading companies.[4] Its goal is to drive the adoption of interoperable wireless solutions in smart cities, smart grids and other IoT applications, based on open and international standards [53].

Here we focus on the FAN (Field Area Network) profile that is akin to the LPWAN set of technologies, but it works on top of IEEE 802.15.4g [63]. Wi-SUN FAN provides a large coverage range of several kilometers, high bandwidth with transmissions up to 300 kbps and low latency. In terms of energy, they require less than 2 uA when resting and 8 mA in listening mode. From a scalability perspective, Wi-SUN networks can support thousands of devices.

Authentication and access control is done using the EAP lower-layer IEEE802.1x, also known as EAPOL, with the EAP-TLS method. To support muti-hop scenarios, when the EAP peer is not able to reach the EAP authenticator by its own means, the EAPOL datagram can be forwarded by multiple routing nodes. Additionally, FAN nodes support Node Pairwise (N2NP) Authentication [64] among neighbors in the mesh. Furthermore, FAN integrates additional protocols and methods for managing the network access exploiting EAP, which brings the possibility of an easier integration within a 5G infrastructure.

[3] https://www.sigfox.com/en/coverage

[4] https://wi-sun.org/

F. ANALYSIS OF RESEARCH PROPOSALS

As previously mentioned, the security limitations of current LPWAN technologies have attracted a significant interest from both industry and academia in recent years. In addition to the security aspects of the technology itself, the integration with the 5G ecosystem represents a new challenge in terms of interoperability with 5G security technologies. This section describes the main research proposals addressing security issues in the LPWAN technologies described above. Additionally, our analysis explores security approaches for the integration of each LPWAN technology within the 5G architecture.

In the case of LoRaWAN, the limitations on its key management scheme have been widely reported by different works. As discussed by [65], in the LoRaWAN 1.0 specification [56], the *network server* is responsible for generating the NwkSKey and AppSKey session keys even if they are used at different layers. It means that the *network server* could have access to the application data sent by the device. To cope with this issue, authors describe a dual key-based activation scheme, so that *network server* and *application server* use different keys to generate the corresponding session keys. Therefore, key management is separated between network and application layers. This aspect is also addressed in [66], which proposes a security protocol to provide end-to-end security between device and the *application server*. Authors validated their proposal by using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [67], and provided some evaluation results, which are compared with the Datagram Transport Layer Security (DTLS) [68]. Furthermore, [69] proposed the use of the Ephemeral Diffie-Hellman Over COSE (EDHOC) [70], which represents a standardisation effort for a lightweight authenticated key exchange protocol in the scope of the IETF's LAKE WG.[5] In this case, the NwkSKey and AppSKey session keys are updated/refreshed through the execution of such protocol. A different approach was proposed in [71], which presents an enhanced key management and update approach by adding a trusted key distribution server in the context of smart grid scenarios [72].

An additional issue identified in [65] is that LoRaWAN 1.0 does not define any mechanism to update the initial AppKey. This means that such key can be used throughout the whole device's lifecycle, which may represent a significant security issue if it compromised as the attacker could obtain all the previous session keys. In this direction, work in [73] defined an authentication service (Low-Overhead CoAP-EAP (LO-CoAP-EAP)) to generate an AppKey based on the integration of three main technologies: the Constrained Application Protocol (CoAP) [74], the Extensible Authentication Protocol [75], and the use of AAA infrastructures. This approach represents an adaptation of the solution proposed in [76] for LoRaWAN networks. The same authors also defined a mechanism to integrate the LoRaWAN join procedure with AAA for RADIUS and Diameter protocols [77]–[79]. This proposal provides several advantages in terms of scalability, efficiency and flexibility. Furthermore, the use of EAP and AAA could foster its integration into the 5G architecture, which defines an authentication process based on such technologies, as described in the previous section. While previous issues are partially mitigated by the LoRaWAN 1.1 specification [57], security aspects of the new release have also been discussed by recent works [80]. In this line, authors of [81] analysed key management aspects of the LoRaWAN 1.1 join procedure, and discussed several issues around perfect forward secrecy and backward compatibility. Moreover, work in [82] described an enhanced key management scheme to update the root keys, i.e., AppKey and NwkKey, by using the Rabbit cipher scheme [83]. Furthermore, work in [84] proposed the addition of a trusted third party for the generation of session keys. Also addressing key management aspects, [85] proposes a re-keying approach to ease the deployment of LoRaWAN devices in which a smartphone's camera flash is employed to transfer the necessary credentials.

In addition to key management, other LoRaWAN security issues are addressed by other works. In this direction, work in [86] presented a replay attack prevention scheme for the join mechanism, which follows the standard packet structure. In particular, authors added a new non-initial join request, in which the NwkSKey is used by the *network server* to detect replay attacks, as it changes for each request. Moreover, authors of [87] defined a secure device-to-device link establishment scheme based on two new messages to allow secure communications between devices. Furthermore, the integration of distributed ledger technology [88] has been considered in [89] to cope with the centralized nature of LoRaWAN network servers. Specifically, authors proposed a two-factor authentication approach for the join procedure, in which the information of EDs is stored in a simulated blockchain by using Ethereum [90]. Furthermore, authors of [91] proposed a permissioned blockchain, in which smart contracts are used for key management aspects. A similar approach is also designed in [92] in which *network servers* were extended with blockchain functionality.

More focused on the integration of LoRAWAN within the 5G architecture, work in [93] analyzed the role of LPWAN in 5G by presenting a performance analysis for LoRaWAN in terms of coverage and throughput. Authors identified some potential issues of such integration specially related to scalability. Moreover, a discussion regarding the integration of LoRaWAN into 4G/5G for industrial IoT scenarios was presented in [94]. Authors also proposed an approach in which only LoRaWAN gateways need to be modified. Moreover, work in [95] addressed mobility aspects through a handover roaming mechanism for LoRaWAN, where devices can use 5G or LoRaWAN authentication to enable interoperability between both technologies. Authors also implemented and validated their solution in an integrated 5G-LoRaWAN testbed.

[5] https://datatracker.ietf.org/wg/lake/about/

In the case of NB-IoT, authors of [59] identified several security attacks including resource exhaustion, selective forwarding or Distributed Denial-of-Service (DDoS) attacks. They also proposed several security countermeasures in the scope of different scenarios, such as smart healthcare or smart agriculture. Security threats and attacks in NB-IoT are also discussed by [96], which defines an architecture to demonstrate the possibility of launching certain attacks on a NB-IoT network. Furthermore, the work in [97] described a differential radio frequency watermark approach to mitigate several security attacks and eavesdropping based on computations over the received signals. This approach represents an alternative solution to well-known network or application layer solutions.

Other papers focused on the authentication aspects of NB-IoT by proposing different mechanisms to make the authentication process more efficient specially in the cases with a high number of devices. In this line, authors of [62] reported the overhead required by authentication mechanisms, e.g., 5G-AKA, by describing a fast access mutual authentication and data distribution scheme with quantum attacks resistance. Furthermore, work in [98] proposed a multi-party authenticated encryption scheme without certificates, which is used by NB-IoT devices to be authenticated through their serial number. The proposal also exploits a data aggregation technique to reduce communication overhead. Also based on an authentication scheme without certificates [99], a mechanism to enable the simultaneous authentication of several NB-IoT devices was proposed in [60]. Specifically, this work considered an entity called *group leader*, which aggregates the authentication information of a certain group of devices to be sent to the Mobility Management Entity (MME). Also focused on authentication, authors of [100] proposed the use of LO-CoAP-EAP [73] for the initial authentication of NB-IoT devices. This solution combines the use of the EAP framework and CoAP [74] to realize a lightweight and efficient approach. Moreover, the use of physical unclonable functions (PUF) [101] was considered in [102] to complement the key derivation process between NB-IoT devices and smart grid platforms. A similar approach was also proposed in [103] by using the concept of PUF.

In addition to authentication aspects, additional NB-IoT security concerns have been addressed by additional works. Work in [104] proposed a trust and reputation model based on social aspects of IoT devices [105], in such a way that the definition of a new topology takes the model's values into account. Moreover, authors of [106] integrated SDN and NFV concepts to design an automated deployment of virtual firewalls to protect NB-IoT communications. Besides, in [107] an efficient traffic filtering approach for encapsulated traffic was proposed in order to address mobility requirements of 5G networks based on NB-IoT devices.

Although Sigfox and Wi-SUN FAN technologies are also considered in RFC 8376 [52], they have received less attention in the related literature in order to be integrated within the 5G ecosystem. In the case of Sigfox, this may be due to the fact that it is defined as a closed system, so that it is difficult to design and develop further improvements devoted to increase its robustness or performance. Even so, one proposal addressing security aspects was represented in [108], which discussed the general aspects of Sigfox security and provided a comparison of different encryption techniques, such as AES, Chacha [109], and one time pad encryption [110] when combined with this technology. As mentioned above, Sigfox is included in the RFC 8376, where three main LPWAN areas are identified to be further developed, namely, (i) management features, (ii) security features, and (iii) applications profiles. The initial defined considerations regarding authentication and authorization at large scale, and the implications on key management could be extended to enhance Sigfox in such security aspects. In terms of suitability for integration in 5G networks, Sigfox does not use protocols and technologies that are natively used in 5G for network access. As stated in [111], Sigfox is understood as a technology to coexist with 5G, but as a complementary technology.

Finally, regarding Wi-SUN FAN technology, its security aspects have been not considered yet in the related literature. The main reasons are its novelty and that this technology is based on a standardized stack based on well-known standards from the IETF. Therefore, the security issues are already addressed by technologies that have been widely tested and deployed, such as 802.1X or EAP, with EAP-TLS for authentication purposes. Indeed, the use of 802.1X typically is linked to the use of an AAA infrastructure to perform the authentication, which leads to consider that Wi-SUN FAN is able to provide support for AAA infrastructures. This aspect could facilitate the integration of this technology into the 5G ecosystem considering the authentication mechanisms described in Section III.

As already described, the security aspects of LPWAN networks have attracted a significant interest in recent years. However, our analysis shows that there are still few proposals that address such issues considering the integration with the 5G ecosystem. Among the main LPWAN technologies, most of the analyzed works are based on the use of LoRaWAN and NB-IoT. This is mainly because both technologies have public specifications and are receiving a strong support from industry and SDOs. Moreover, it should be noted that most of research proposals focus on authentication and key management aspects. While both are essential to guarantee a secure integration of LPWAN technologies, it is expected an increase of research proposals in the coming years to address other security issues, such as trust management, access control, intrusion detection and privacy [13]. This will require the integration of emerging technologies, such as the use of machine learning techniques [112] to build effective systems for detecting and mitigating security threats in 5G scenarios, or distributed ledger technologies, e.g., blockchain, to foster a more trustworthy integration of end devices. Beyond the specific security-related aspects, the integration of LPWAN networks in the 5G ecosystem sets out significant challenges that

may impact in a potential secure and large-scale 5G deployment. These challenges are described in the next section.

V. OPEN ISSUES AND CHALLENGES

Based on the analysis provided in the previous section, in the following we describe the main open issues and challenges for the integration of LPWAN technologies in the 5G ecosystem.

A. IoT HETEROGENEITY

The vision of IoT includes the interconnection of heterogeneous EDs communicating through low-bandwidth links. This demands novel protocols or mechanisms dealing with this heterogeneity and also guaranteeing the secure and seamless information exchange of EDs [113]. This approach should be maintained when integrating IoT applications in 5G. Thus, this IoT (LPWAN)–5G interconnected environment leverages on the trend of avoiding individual solutions with vendor-specific dependencies, towards novel distributed and inter-operable service ecosystems. Still, compatibility among different-technology LPWAN systems remains as one of the greatest gaps in order to achieve large-scale deployments to enable next-generation applications. This is due to the characteristic heterogeneity of IoT deployments, where establishing communication links between devices connected to different types of networks is required.

Achieving this in LPWAN is complex due to the existing landscape of available communication technologies, where some of them are open solutions while others are closed products. Indeed, authors of [6] conclude that further efforts towards the compatibility among different technologies are needed and a key factor of this process is the adoption and use of standards. To accomplish this, organizations such as the IETF play an important role in the definition of standards and guidelines to provide common foundations to LPWANs. In this line, authors of [114] provided an overview of the status of LPWAN technologies in the IETF. From this paper, it can be extracted that there is a need for homogenizing different aspects of the life-cycle of the IoT devices, such as authentication, authorization and key management, a task that is being tackled by the IETF through its different WGs, as explained later. This work also describes a general architecture that covers common points of the different LPWAN technologies, such as a radio gateway that connects EDs and LPWAN gateways that aggregate the different radio gateways and provide them with connectivity towards the Internet. From this generalization, authors proposed a series of building blocks for the different LPWAN technologies to be used in order to find interoperation points.

Regarding the related efforts of IETF'S WGs mentioned above, the LPWAN WG has developed the Static Context Header Compression (SCHC) scheme [115] that reduces message size and provides fragmentation to make IPv6 and UDP protocols available for LPWAN technologies. Currently, a version of SCHC for CoAP is still under development [116] to apply the SCHC mechanism to the flexible headers of CoAP for achieving more efficient compression ratios. Besides, there is also work in progress to provide SCHC support to specific technologies, namely, Sigfox [117], LoRaWAN [118], and NB-IoT [119]. Once the technologies have the basic communication functionalities, more advance features should be considered such as identity and device management, security, or mobility, among others. Future work of the LPWAN WG may span to more advanced features such as the support of AAA as mentioned in the LPWAN Overview RFC [52], introducing a more centralized security management, and additional features such as identity federation. These novel characteristics are in line with the security architecture used in 5G, where EAP and AAA are adopted to manage the identity and network access for different devices. There are existing proposals in this direction such as the AAA adaptation for LoRaWAN with RADIUS [77] and Diameter [79]. However, the development of these features will not be the focus of the LPWAN WG until the foundations for the communications of LPWAN technologies are completed.

The proliferating LPWAN technologies that are targeted at being eventually integrated within the 5G ecosystem do not currently incorporate inter-vendor or inter-operable functionalities that allow their integration within third-party networks. These mechanisms are key to support the heterogeneous IoT landscape of devices that 5G aims to integrate. It is currently an ongoing effort by the research community and different SDOs to develop non-vendor locking solutions that further support the compatibility among LPWANs. These solutions take advantage from common characteristics of all IoT devices connected through LPWANs, e.g., similar architectural models, critical bandwidth usage, low-overhead standardised protocols to perform security-related network administration tasks, among others. Therefore, we can expect in the near future more advances in the area of security and related fields applied to LPWAN coming from other WGs. A clear example is the work of the IETF's LAKE WG and their use case for LPWAN, where the requirements of a lightweight Authenticated Key Exchange (AKE) for OSCORE are being discussed. One of the studied cases is the use of LoRaWAN, which has also received attention from the research community in similar terms [120].

B. INTEROPERABILITY

Regarding the smoothness in the LPWAN integration process within the 5G architecture, the open or closed nature of the LPWAN solution to be integrated should be considered, e.g., LoRaWAN vs. Sigfox. Besides, the use (or not) of standardised protocols or mechanisms is another issue that should be taken into account to evaluate the complexity of such integration regarding the interoperability between LPWAN and 5G procedures.

Therefore, the desired integration should be free-flowing when dealing with an LPWAN solution based on an open specification using standardised mechanisms. The main concern in this case may be the off-the-shelf compatibility of

the adopted standards with 5G procedures. It is interesting to note that none of the principal LPWAN technologies fall into this category. In turn, LPWAN solutions based on closed specifications but using standards schemes, as long as they were compatible with 5G, should be fairly easy to inter-operate with 5G procedures. This is the case of Wi-SUN, where the customer has no control over the development of the technology or how to customize it, but since they are using standard protocols, the integration with 5G may be reasonably feasible.

In the case of dealing with solutions based on an open specification that makes use of non-standard protocols, an adaptation process should be taken in order to perform the necessary modifications to integrate the technology with 5G. An example of a specific solution customisation is shown in [94], where authors proposed different ways of coupling LoRaWAN with 5G. Lastly, LPWAN solutions based on closed designs that do not use standard procedures are the hardest case as no adaptations would be possible, unless some intermediate entity may assume the role of a interoperability bridge between the proprietary protocol and the 5G infrastructure. This would be the case of Sigfox, where there is no control over the development of the technology and it employs proprietary protocols.

In addition, current IoT ecosystem includes highly closed environments, typical in industrial settings, where many different ad-hoc protocols coexist, forcing vendor-locking architectures and solutions. While there are some efforts related to improve system's scalability or even network federation approaches in specific LPWAN technologies, e.g., LoRaWAN [121], these are usually only compatible with native intra-technology deployments. That means that LPWAN-based solutions do not include in their specifications mechanisms to manage a combined deployment with other technologies, hence the development of interoperable procedures among different LPWAN solutions to integrate them into 5G still remains a great open challenge.

In addition, there are still open issues regarding the mutual lack of trust among 5G Home, Serving, and Access networks. This includes the end-user herself, who may not trust the different network operators due to their particular procedures to manage network security aspects. This is reasonable for certain users and use cases, as the level of security depends on the network operators [44] as discussed in Section III-C. To solve this issue, two different approaches have been proposed in the literature, namely, (i) adding a trusted third-party element to the architecture in charge of managing the security mechanisms [84], and (ii) exploiting a distributed ledger architecture deployed along the different involved parties [89], [91], [122]. Following these proposals, in order to increase the confidence in 5G as a system for critical applications, the potential solutions are based on providing customers with additional trust mechanisms able to handle or bypass potential exploited vulnerabilities on the network operator side.

C. MOBILITY

Mobility in the context of network access is a term that refers to the dynamic change of Point of Attachment (PoA). This generalization can be narrowed by considering if the PoA change is within the same administrative domain or in a different one. When it comes to LPWANs, mobility does not have the typical connotations of cellular networks, where mobility refers to keeping a constant uninterrupted stream of information by performing the handover process without data loss. In contrast, LPWAN traffic is usually devised as small packets of data transmitted at sporadic periods, most of the time in delay tolerant scenarios. Despite this, there are uses cases where mobility is relevant in LPWAN, such as those from Intelligent Transportation Systems (ITS) [123], which consider mobility as a specific need to provide uninterrupted connectivity. Hence, when changing the administrative domain, we find a roaming scenario where it is crucial to account for a specific set of preconditions that need to be met such as pre-established trust relations between the two domains as well as identity management and security specifically associated to this scenario. Some LPWAN technologies present mobility capabilities, even in roaming scenarios, such as LoRaWAN [20]. The main related issue is not having a native support to the technology but an interoperable one, as remarked by Torroglosa-Garcia *et al.* in [95], where they proposed a mobility solution, which employed 5G to provide an interoperable roaming solution, either by running a standard 5G authentication or doing it through a LoRaWAN network.

Therefore, providing EDs with roaming capabilities is a highly discussed 5G security challenge. This is because the user security parameters are not updated when visiting a new administrative domain, leading to a trade-off between access security and roaming capabilities [124]. Some of the limitations to the deployment of a roaming solution is the lack of pre-existing trust agreements among the different administrative domains. This process is typically performed by relying on AAA infrastructures, where the mobile node (MN) in a visiting network delegates the authentication process to the local AAA server, which in turn forwards the request to the home AAA of the MN. To enable this process, the integration of AAA within LPWAN solutions is needed. Some of them such as Wi-SUN provide native support by their native stack, although it can be limited by the manufacturer's design. The are additional proposals for other LPWAN technologies, e.g., LoRaWAN, such as the IETF's I-D from Garcia-Carrillo *et al.* [77] where they propose the integration of the LoRaWAN joining procedure within RADIUS and Diameter architectures.

D. SCALABILITY

Many 5G security challenges in IoT scenarios identified by the research community are tightly related to scalability. This includes flash or surge network traffic in massive

IoT deployments, radio link jamming, signalling storms, Denial-of-Service (DoS) attacks aimed at constrained EDs, DDos attacks coming from EDs, etc. [125]. Scalability has several connotations, in this case for LPWAN we focus on the issues to support a large number of devices within a single deployment, which has its own inherited limitations due the physical characteristics of the radio technology, and also the constraints caused by the duty-cycle imposed to LPWAN technologies that use ISM bands. Besides, we also consider the interoperability factor, which is the main effort within the IETF's LPWAN WG as explained previously. To provide such interoperability, not just the homogenization of communications protocols should be considered, as elaborated in section V-A, but also security aspects such as user authentication and authorization as well as key agreement and distribution should be taken into account. These aspects were previously discussed in section V-C.

The use of AAA infrastructures does not only fit in the mobility use case, but also helps establishing the necessary trust relationships between different domains. This paves the way for having large-scale deployments similar to mobile network systems, supporting a high number of devices and, at the same time, giving the possibility of using different authentication mechanisms if coupled with protocols such as EAP [73]. Therefore, regardless the underlying authentication mechanism used for network access, the use of a centralized entity, e.g., LPWAN-AAA using the terminology in [46], will open a range of opportunities for managing security procedures in large-scale IoT deployments.

Consequently, the scalability problem presented by massive IoT scenarios, such as those accommodated by LPWANs, revolves around the management issues brought by the desired support for different security procedures and types of keys. One single administrative domain must support a daunting amount of devices, many of them with their own set of keys and trust relationships. In order to mitigate these administrative problems, the major research and standardisation efforts are those focused towards centralised and scalable AAA architectures that facilitate management tasks.

E. PERFORMANCE

Most of the security concerns found in LPWAN scenarios are related with radio attacks in the constrained wireless link. Given the wide coverage area of LPWANs, the available geographical locations are prone to allow attacks such as eavesdropping, DoS, tampering, etc. LPWANs are characterized by the limitation of available bandwidth and restricted access to the medium, which evidences the need for security solutions, e.g., bootstrapping, authentication and key agreement protocols, etc., that put an effort in limiting the number of information to be exchanged. In contrast, the use of typical security protocols such as IKE, TLS, or even DTLS in its previous version DTLSv1.2, implies an important overhead in terms of exchanged cryptographic data [126] that may be unaffordable for LPWAN solutions. Besides, one remaining challenge for 5G-LPWAN integration consists in developing a set of optimised downlink multicast methods required to transmit the same data to a large set of IoT devices. Besides the obvious improvement of network efficiency, multicast transmissions are also relevant in a security context, due to the possibility of simultaneously authenticating large groups of IoT devices [36].

From a processing perspective, computing power is limited due to the constrained nature of EDs, hence strong cryptographic primitives that require large amounts of time and energy to be performed are prohibitive. As aforementioned, different works suggest the use of alternative cryptographic schemes to avoid heavy computations [102], [103]. However, there is still a notable need for mechanisms that enhance lightweight security features without the expense of excessive energy consumption and economic cost for LPWAN systems. Interesting related advances are being achieved in other fields such as the TinyML paradigm [127], which proposes to adapt powerful machine learning mechanisms in order to make them runnable by constrained IoT devices. In fact, some of the identified potential applications are oriented to on-device security operations [128].

Currently, there are ongoing initiatives that are having these issues into account and are designing new security protocols to provide lightweight alternatives devoted to highly constrained networks and devices. These are the cases of Compact TLS (CTLS) [129] and EDHOC, recently adopted in TLS and LAKE WGs, respectively. This shows not only an interest, but a serious effort to provide security to these type of networks. It can be seen that there is a clear line of research and innovation in this area, developing authentication protocols or solutions to help not only in the reduction of the communication and processing overheads, but also providing interoperability and flexibility to this process in the LPWAN landscape.

VI. RESEARCH DIRECTIONS

Based on our analysis and the challenges previously described, in this section we describe some of the main research directions to deal with such challenges. In particular, we consider the integration with emerging technologies, as well as the advances derived from ongoing standardisation efforts and current EU initiatives to foster a large-scale and secure 5G deployment.

A. INTEGRATION WITH EMERGING PARADIGMS

The integration of heterogeneous IoT systems within 5G architectures may be smoother by the support of novel paradigms such as Multi-access Edge Computing (MEC), Software Defined Networks (SDN), Network Function Virtualization (NFV), or advanced RAN management schemes. The flexibility provided by these technologies can notably help on giving an adequate treatment to the traffic flows generated by massive IoT deployments, specially from a cyber-security perspective.

Adopting a MEC architecture is beneficial as it permits to set a first point of connection between EDs and the fixed

network infrastructure. For example, performing traffic flow inspection in this specific point prevents dangerous deep intrusions into the 5G infrastructure. This point may be also in charge of forwarding authentication messages to the proper AAA server in the case of having a multi-tenancy system [130]. In general, MEC nodes can offload or filter many operations that are currently performed in the core network, hence reducing the load in this saturated segment of the system.

Besides, the use of SDN-based routing approaches also permits a flexible management of traffic flows by making smart decisions from a central controller with a general perspective of the whole network architecture. This can be exploited for security purposes, as malicious traffic, e.g., Denial-of-Service (DoS) attack, can be quickly redirected avoiding catastrophic consequences. SDN can be complemented with other useful traffic management and security functions that can be instantiated on-demand in the form of VNFs [131]. The main advantage of VNFs is that these functions can be deployed at any level of the network architecture when needed for performing specific tasks, e.g., threat detection and mitigation, firewalling, AAA verification, etc. Besides, these novel paradigms can be additionally complemented with the use of blockchain-based trust systems in order to increase the auditability and accountability of the data transactions and operations [122].

Finally, from a RAN perspective, the use of advanced highly selective beamforming or even cognitive radio techniques may also permit to increase the robustness of IoT wireless communications against different types of radio attacks [132]. For example, by avoiding widespread omnidirectional transmissions, the possibilities of suffering an eavesdropping attack are notably reduced. Besides, an adequate channel-hopping strategy may also avoid these kinds of attacks, specially during the authentication phase, when initial messages may be sent unprotected.

B. STANDARDIZATION

The current landscape of technologies and protocols enabling the 5G ecosystem is still fragmented. For this reason, the main Standards Developing Organizations (SDOs) have proposed different initiatives in recent years to promote a security by-design development based on a common understanding, in order to achieve a large-scale 5G deployment. The main body working on the standardization of 5G is the 3rd Generation Partnership Project (3GPP),[6] which groups different SDOs to provide specifications on 3GPP technologies. In particular, 3GPP is divided into different Technical Specification Groups (TSGs) focused on RAN, services and systems (SA), and network and core terminals (CT). 3GPP launched in 2019 the first set of 5G standards (3GPP release 15) in which security is considered in different documents. In addition to the ''Security architecture and procedures for 5G System'' [32] specification, which has been partially described in Section III, additional reports provide different perceptions of security aspects to be considered in 5G deployments. In this direction, the SA3 working group has elaborated the ''Study on security aspects of 5G network slicing management'' [133], which analyzes the threats and potential security requirements of 5G network slicing. Other specifications address additional security aspects, such as the ''Study on security aspects of the 5G Service Based Architecture (SBA)'' [134] which identifies key security concerns in a new service-based architecture for 5G. In addition, the recent release 16 delves into aspects about the integration of IoT into the 5G ecosystem and the corresponding security aspects.[7]

In addition to 3GPP, standardization in 5G has attracted a significant interest from other SDOs. On the one hand, the Next Generation Mobile Networks (NGMN) Alliance[8] is intended to define requirements for 5G systems, as well as to provide guidelines for potential standardization activities. In fact, NGMN published in 2015 a white paper with an exhaustive set of requirements for the development of 5G, including security, privacy, virtualization, and IoT aspects [125]. On the other hand, the study group ''SG17: Security'' of the ITU Telecommunication Standardization Sector (ITU-T)[9] is focused on the security aspects of communication and information technologies. In particular, the group considers security aspects in 5G through the topic ''Security aspects of telecommunication services, networks and Internet of Things'',[10] which addresses research and development of standards on security and privacy features of 5G services.

Furthermore, European Telecommunication Standards Institute (ETSI) has different working groups related to technologies that are intended to be part of the 5G ecosystem (see Section V-A). Thereby, the ETSI NFV[11] is focused on the standardization of SDN and NFV technologies, as well as the associated security aspects. Besides, the ETSI ISGN MEC is intended to create a standardised environment for MEC technologies in order to foster seamless integration. Finally, the ETSI TC CYBER[12] is focused on the development of standards for cybersecurity. As part of its activities, security aspects in 5G are mentioned in [135], where attribute-based encryption (ABE) is considered to protect personal data. Also focused on the security capacities of SDN, the Open Networking Foundation (ONF)[13] being a non-profit organization has promoted the development of SDN and its integration into 5G scenarios, such as in the case of network slicing [136].

Additionally, while the IETF does not have specific initiatives focused on 5G, the contributions of different working

[6] https://www.3gpp.org/dynareport/SpecList.htm?release=Rel15&tech=4

[7] https://www.3gpp.org/release-16

[8] https://www.ngmn.org/

[9] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

[10] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/q6.aspx

[11] https://www.etsi.org/technologies/nfv

[12] https://www.etsi.org/committee/cyber

[13] https://www.opennetworking.org/mission/

groups can be considered in diverse technologies composing the 5G ecosystem. Apart from the working group for LPWAN networks (IPv6 over Low Power Wide-Area Networks),[14] the Authentication and Authorization for Constrained Environments (ACE) WG[15] is focused on adapting authentication technologies and authorization environments with devices and restricted networks. In addition, the recent establishment of the Lightweight Authenticated Key Exchange (LAKE) WG[16] provides a LAKE protocol for constrained environments. The solutions of these working groups could be applied in the context of LPWAN networks in order to improve the security aspects of these technologies. Indeed, our previous work about key management in LoRaWAN [69] proposes the use of the Ephemeral Diffie-Hellman over COSE (EDHOC) [70], [137], which is being currently defined in the scope of the ACE WG.

In the light of the previous discussion, it is clear the great interest from SDOs in the further development of IoT security mechanisms for making them compatible with 5G security procedures. While 3GPP is the main SDO defining the 5G architecture, others such as NGMN, ITU, and ETSI are proposing security enhancements and compatibility solutions to integrate other network access technologies within 5G systems. Besides, the specific efforts of IETF on the development of lightweight security schemes paves the way for their implementation on constrained IoT devices hence providing them with the required security capabilities as any other 5G UE. Thus, given these efforts from prominent SDOs, we envision a highly promising near future in which the convergence between IoT and 5G will become a fruitful reality.

C. 5G INITIATIVES IN THE EU

In recent years, the development of 5G technologies has been widely considered as one of the main enablers of future digital services. The European Commission (EC) has launched ambitious initiatives to support the cooperation among stakeholders in different Member States (MSs) for the development of 5G-enabled services. These initiatives include the 5G Action Plan,[17] which represents a strategic effort to align roadmaps and priorities for a coordinated 5G deployment across the EU. Furthermore, the 5G Infrastructure Public Private Partnership (5GPPP)[18] is a joint initiative between the EC and EU industry (including telecommunications operators, SMEs or research institutes) to foster a common vision about 5G developments in the EU. Indeed, the development of 5G is widely considered as crucial to ensure the strategic autonomy of the EU.

In this context, previous initiatives consider cybersecurity as a critical aspect for the deployment of 5G in the EU. In fact, it is expected that 5G technologies will play a key role in the Digital Single Market (DSM) with a strong impact in several scenarios, such as energy, transport, or health services. Moreover, 5G will enable a more interconnected world, where vulnerabilities of 5G systems in a single member state could affect the EU as a whole. Therefore, there is a need to promote collaboration and cooperation among countries to support a coordinated and secure deployment of 5G. To address such need, the EC launched the Recommendation ''Cybersecurity of 5G networks''[19] in 2019 to propose a set of concrete actions for ensuring cybersecurity of 5G networks, including the development of national risk assessment strategies of 5G infrastructures. The main goal is to leverage national efforts to develop a coordinated EU risk assessment, in order to create a common toolbox of best risk management measures. As part of these efforts, the ''EU coordinated risk assessment of the cybersecurity of 5G networks'' report [138] identifies the main threats, sensitive assets, vulnerabilities and associated risks of 5G networks. This report was used together a recent ENISA report on 5G threats [139] to create the initial version of the mentioned toolbox.

To ensure the development of secure 5G deployments, cybersecurity certification is essential to promote a transparent and trustworthy ecosystem of 5G devices and systems. The new EU cybersecurity regulation ''Cybersecurity Act'' entered into force in 2019 to create a cybersecurity certification framework for any ICT product, service or process. It complements the existing GDPR and NIS Directive to strengthen the cybersecurity in the EU. Indeed, it is expected that the Cybersecurity Act plays a key role in the development of 5G technologies. As described in the already mentioned Recommendation ''Cybersecurity of 5G networks'', the realization of such framework is an essential tool to promote consistent levels of security and the creation of certification schemes adapted to 5G related equipment. Furthermore, the mentioned toolbox identifies the EU certification for 5G network components, customer equipment and/or suppliers' processes as one of the main technical measures to strengthen the security of 5G networks. In this direction, a common understanding of the threats, assets, attacks and risks of 5G systems is essential to create a certification scheme that could help to recognize the security level of a certain 5G system across all the member states. Toward this end, the outcomes of existing initiatives, such as the creation of a EU risk assessment strategy could help to reach such harmonized view.

Besides the already mentioned initiatives, in recent years the EU has funded several research projects in the scope of the Horizon H2020 programme. Indeed, there are currently several ongoing efforts dealing with the convergence of IoT and 5G ecosystems, such as COREnect [140], which is intended to develop a roadmap of core technologies for 5G and beyond. More focused on specific use cases and scenarios, 5G-LOGINNOV [141] deals with the integration of 5G in several applications, such as Industry 4.0 and Cooperative Intelligent Transport Systems (C-ITS). This scenario

[14] https://datatracker.ietf.org/wg/lpwan/about/
[15] https://datatracker.ietf.org/wg/ace/about/
[16] https://datatracker.ietf.org/wg/lake/about/
[17] https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan
[18] https://5g-ppp.eu/
[19] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

is the main topic of the 5G-MOBIX project [142], which aims at developing automated vehicle functionalities, such as cooperative overtake, truck platooning, valet parking, road user detection, vehicle remote control, HD map update and media & entertainment by using 5G core technological innovations along multiple cross-border corridors and different urban settings. Moreover, other projects are focused on certain technologies to foster the integration of IoT devices into the 5G ecosystem. In this direction, Int5Gent [143] works on a 5G-system platform to validate 5G services and IoT solutions. In particular, the project is intended to integrate a slice and application orchestration framework based on SDN, NFV and edge computing to provide such platform. These aspects are also addressed in the scope of the 5G-DIVE [144] project, which is focused on the integration of edge/fog computing and orchestration systems to build an end-to-end network testing platform for 5G systems. Furthermore, 5G-COMPLETE [145] deals with the integration of computing and storage functionality over a fiber-wireless radio access network by using post-quantum crypto-systems for security encryption. More focused on security management, INSPIRE-5Gplus [146] is currently implementing a fully automated end-to-end smart network and service security management framework that empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across multiple domains, including IoT systems. Moreover, SPIDER [147] is working on a replicable cyber range platform for 5G systems by providing cybersecurity emulation tools, novel training methods based on active learning as well as econometric models based on real-time emulation of modern cyber-attacks.

As we can see there is a clear interest in the development of 5G solutions and their relation to different branches of the IoT ecosystem. However, based on our analysis, still there is a lack of specific initiatives coping with the security concerns associated to LPWAN-enabled devices and their integration in 5G systems. These aspects need to be considered in the coming future to deal with the heterogeneous nature of such devices, and the requirements about lightweight, flexible and scalable security mechanisms.

VII. CONCLUSION

The great interest in the convergence of IoT and 5G ecosystems has fueled the development of standards, industrial solutions and research proposals for solving the security issues that this complex integration brings. This paper has deeply reviewed the security procedures of the 5G architecture, as defined by the 3GPP standard, and explored the security strengths and weaknesses of widely adopted LPWAN-based technologies such as LoRaWAN, Sigfox, or NB-IoT. From this discussion, it can be concluded that current security schemes employed in LPWAN-based solutions require additional enhancements and adaptations for complying with 5G network-access requirements. In this line, many initiatives to solve these issues can be found in the literature. Different SDOs such as ITU or IETF are proposing concrete actions for the smooth integration of both ecosystems, with interesting efforts from the latter in the development of lightweight security protocols for IoT EDs. Many proposals from the academia and ongoing projects have been also reviewed, showing the great momentum of this hot topic, which augurs a successful evolution of IoT systems and their security mechanisms to be compliant with the stringent 5G security requirements. However, for this to be done, some additional steps should be taken. Firstly, the adoption of novel paradigms such as network virtualisation, i.e., SDN and NFV, or MEC will be of great help for a seamless interoperability of heterogeneous IoT systems among themselves and with the 5G infrastructure. Secondly, the additional development of simple but robust network access procedures is crucial for enabling constrained IoT EDs to perform lighter cryptographic operations as well as exchanging a reduced number of messages. Finally, the massive and dynamic nature of certain IoT deployments call for solutions to ensure the system scalability and the mobility of EDs by means of novel simple roaming mechanisms.

REFERENCES

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
[2] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
[3] S. K. Sharma and X. Wang, "Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 426–471, 1st Quart., 2020.
[4] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Exp.*, vol. 5, no. 1, pp. 1–7, Mar. 2019.
[5] S. Bocker, C. Arendt, P. Jorke, and C. Wietfeld, "LPWAN in the context of 5G: Capability of LoRaWAN to contribute to mMTC," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 737–742.
[6] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77454–77473, 2018.
[7] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.
[8] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for IoT applications," *Telecommun. Syst.*, vol. 71, no. 2, pp. 249–274, Jun. 2019. [Online]. Available: http://link.springer.com/10.1007/s11235-019-00557-9 and doi: 10.1007/s11235-019-00557-9.
[9] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8879484/
[10] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8894379/
[11] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8792139/
[12] S. Zhang, Y. Wang, and W. Zhou, "Towards secure 5G networks: A survey," *Comput. Netw.*, vol. 162, Oct. 2019, Art. no. 106871. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S138912861830817X and doi: 10.1016/j.comnet.2019.106871.

[13] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the Internet of Things era: An overview on security and privacy challenges," *Comput. Netw.*, vol. 179, Oct. 2020, Art. no. 107345. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128620300827

[14] R. Fujdiak, K. Mikhaylov, M. Stusek, P. Masek, I. Ahmad, L. Malina, P. Porambage, M. Voznak, A. Pouttu, and P. Mlynek, "17–Security in low-power wide-area networks: state-of-the-art and development toward the 5G," in *LPWAN Technologies for IoT and M2M Applications*, B. S. Chaudhari and M. Zennaro, Eds. New York, NY, USA: Academic, 2020, pp. 373–396. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128188804000181

[15] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–5.

[16] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J.-P. Koskinen, "Overview of narrowband IoT in LTE rel-13," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2016, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/7785170/

[17] Y.-P.-E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3GPP narrowband Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 117–123, Mar. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7876968/

[18] J. Schlienz and D. Raddino, "Narrowband Internet of Things whitepaper," Rohde&Schwarz, New Delhi, India, White Paper 1MA266_0e, 2016, pp. 1–42.

[19] Y. D. Beyene, R. Jantti, O. Tirkkonen, K. Ruttik, S. Iraji, A. Larmo, T. Tirronen, and A. J. Torsner, "NB-IoT technology overview and experience from cloud-RAN implementation," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 26–32, Jun. 2017.

[20] L. Alliance, "What is it LoRaWAN—A technical overview of LoRa and LoRaWAN," LoRa Alliance, Fremont, CA, USA, Tech. Rep. v1.0, Nov. 2015. [Online]. Available: https://lora-alliance.org/resource-hub/what-lorawantm

[21] J. C. Zuniga and B. Ponsard, *Sigfox System Description*, LPWAN@ document IETF97, Nov. 2016.

[22] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, *Smart Cities: Foundations, Principles, and Applications*. Hoboken, NJ, USA: Wiley, 2017.

[23] J. L. Hernandez-Ramos, J. A. Martinez, V. Savarino, M. Angelini, V. Napolitano, A. Skarmeta, and G. Baldini, "Security and privacy in Internet of Things-enabled smart cities: Challenges and future directions," *IEEE Secur. Privacy*, early access, Aug. 2020, doi: 10.1109/MSEC.2020.3012353.

[24] S. Farahani, *ZigBee Wireless Networks and Transceivers*. Oxford, U.K.: Newnes, 2011.

[25] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, vol. 43. Hoboken, NJ, USA: Wiley, 2011.

[26] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 1, pp. 383–398, Jan. 2019.

[27] O. Hamdi, M. A. Chalouf, D. Ouattara, and F. Krief, "EHealth: Survey on research projects, comparative study of telemonitoring architectures and main issues," *J. Netw. Comput. Appl.*, vol. 46, pp. 100–112, Nov. 2014.

[28] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[29] M. S. Mekala and P. Viswanathan, "A survey: Smart agriculture IoT with cloud computing," in *Proc. Int. Conf. Microelectronic Devices, Circuits Syst. (ICMDCS)*, Aug. 2017, pp. 1–7.

[30] S. Kent and K. Seo, "Security architecture for the Internet protocol," Internet Eng. Task Force (IETF), Fremont, CA, USA, Tech. Rep. RFC4301, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4301

[31] A. R. Prasad, "3GPP 5G Security," Tech. Rep., Oct. 2018. [Online]. Available: https://www.3gpp.org/ftp/Information/presentations/presentations_2018/2 018_10_17_tokyo/presentations/2018_1017_3GPP%20Summit_06_5G%20Security_Prasad.pdf

[32] *Security architecture and procedures for 5G System*, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) document 33.501, version 15.5.0. [Online]. Available: http://www.3gpp.org/DynaReport/33501.htm

[33] J. Arkko, V. Lehtovirta, and P. Eronen, *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')*, RFC, document 5448, May 2009. [Online]. Available: https://rfc-editor.org/rfc/rfc5448.txt

[34] D. Simon, R. Hurst, and D. B. D. A. D. Ph, "The EAP-TLS Authentication Protocol," *RFC*, vol. 5216, Mar. 2008. [Online]. Available: https://rfc-editor.org/rfc/rfc5216.txt

[35] B. Aboba, L. Blunk, J. Vollbrecht, and J. Carlson, "Extensible authentication protocol (EAP)," Internet Eng. Task Force (IETF), Fremont, CA, USA, Tech. Rep. RFC3748, Jun. 2004. [Online]. Available: https://www.rfc-editor.org/info/rfc3748

[36] D. Chandramouli, R. Liebhart, J. Pirskanen, G. Choudhary, J. Kim, and V. Sharma, *5G for the Connected World*, vol. 9, no. 4. Hoboken, NJ, USA: Wiley, 2019.

[37] M. Condoluci, S. H. Johnson, V. Ayadurai, M. A. Lema, M. A. Cuevas, M. Dohler, and T. Mahmoodi, "Fixed-mobile convergence in the 5G era: From hybrid access to converged core," *IEEE Netw.*, vol. 33, no. 2, pp. 138–145, Mar. 2019.

[38] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, *Internet Key Exchange Protocol Version 2 (IKEv2)*, RFC document 7296, Oct. 2014. [Online]. Available: https://rfc-editor.org/rfc/rfc7296.txt. [Online]. Available: https://www.rfc-editor.org/info/rfc7296

[39] R. Housley and B. Aboba, *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management*, RFC document 4962, 2007. [Online]. Available: https://tools.ietf.org/html/rfc4962

[40] *Service requirements for next generation new services and Markets*, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) document 22.261, version 16.8.0. [Online]. Available: http://www.3gpp.org/DynaReport/22261.htm

[41] M. Sethi, B. Sarikaya, and D. Garcia-Carillo. (2020). *Secure IoT Bootstrapping: A Survey, Internet Engineering Task Force, Internet-Draft Draft-Sarikaya-t2trg-Sbootstrapping-08*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-sarikaya-t2trg-sbootstrapping-08

[42] P. Wouters, H. Tschofenig, J. Gilmore, S. Weiler, and T. Kivinen, *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, RFC, document 7250, 2014. [Online]. Available: https://rfc-editor.org/rfc/rfc7250.txt

[43] T. Aura and M. Sethi. (2020). *Nimble out-of-Band Authentication for EAP (EAP-NOOB), Internet Engineering Task Force, Internet-Draft Draft-Aura-Eap-Noob-08*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-aura-eap-noob-08

[44] A. Kunz and X. Zhang, "New 3GPP security features in 5G phase 1," in *Proc. IEEE Conf. Standards for Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–6.

[45] D. Garcia-Carrillo, R. Marin-Lopez, A. Kandasamy, and A. Pelov, "A CoAP-based network access authentication service for low-power wide area networks: LO-CoAP-EAP," *Sensors*, vol. 17, no. 11, p. 2646, Nov. 2017.

[46] K. S. Garcia-Morchon, "Internet of Things (IoT) security: State of the art and challenges," Internet Eng. Task Force (IETF), Fremont, CA, USA, Tech. Rep. RFC8576, 2019.

[47] F. Montori, L. Bedogni, M. Di Felice, and L. Bononi, "Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues," *Pervas. Mobile Comput.*, vol. 50, pp. 56–81, Oct. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1574119217303668 and doi: 10.1016/j.pmcj.2018.08.002.

[48] G. Ergeerts, M. Nikodem, D. Subotic, T. Surmacz, B. Wojciechowski, P. De Meulenaere, and M. Weyn, "DASH7 alliance protocol in monitoring applications," in *Proc. 10th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC)*, Nov. 2015, pp. 623–628.

[49] W. Webb, *Understanding Weightless: Technology, Equipment, and Network Deployment for M2M Communications in White Space*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[50] S. Lippuner, B. Weber, M. Salomon, M. Korb, and Q. Huang, "EC-GSM-IoT network synchronization with support for large frequency offsets," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[51] P.-C. Hsieh, Y. Jia, D. Parra, and P. Aithal, "An experimental study on coverage enhancement of LTE cat-M1 for machine-type communication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–5.

[52] S. Farrell, *Low-Power Wide Area Network (LPWAN) Overview*, RFC, document 8376, May 2018. [Online]. Available: https://rfc-editor.org/rfc/rfc8376.txt

[53] W.-S. Alliance. (2018). *Wi-SUN Alliance and FAN–Secure Large-Scale IoT Networking for Today and Tomorrow*. [Online]. Available: https://wi-sun.org/wp-content/uploads/Wi-SUN-Alliance-and-FAN.pdf

[54] N. Gondchawar and R. Kawitkar, "IoT based smart agriculture," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 6, pp. 838–842, 2016.
[55] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *J. Ind. Inf. Integr.*, vol. 10, pp. 10–19, Jun. 2018.
[56] *LoRaWAN 1.0 Specification*, LoRa Alliance, Fremont, CA, USA, 2015.
[57] *LoRaWAN 1.1 Specification*, LoRa Alliance, Fremont, CA, USA, 2017.
[58] H. Holma, A. Toskala, and J. Reunanen, *LTE Small Cell Optimization: 3GPP Evolution to Release 13*. Hoboken, NJ, USA: Wiley, 2016.
[59] V. Kumar, R. K. Jha, and S. Jain, "NB-IoT security: A survey," *Wireless Pers. Commun.*, vol. 113, pp. 2661–2708, Apr. 2020.
[60] J. Cao, P. Yu, M. Ma, and W. Gao, "Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1561–1575, Apr. 2019.
[61] F. Ghavimi and H.-H. Chen, "M2M communications in 3GPP LTE/LTE–A networks: Architectures, service requirements, challenges, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 525–549, 2nd Quart., 2015.
[62] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9794–9805, Dec. 2019.
[63] H. Harada, K. Mizutani, J. Fujikawa, K. Mochizuki, K. Obata, and R. Okumura, "IEEE 802.15. 4g based Wi-SUN communication systems," *IEICE Trans. Commun.*, vol. 100, no. 7, pp. 1032–1043, 2017.
[64] ETSI Technical Committee Electromagnetic Compatibility and Radio Spectrum matters (ERM), "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Smart metering wireless access protocol; Part 2: Data link layer (MAC Sub-layer), version 1.1.1," European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France, Tech. Rep. TS 102 887-2, 2013. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102800_102899/10288702/01.01.01_60 /ts_10288702v010101p.pdf
[65] J. Kim and J. Song, "A dual key-based activation scheme for secure LoRaWAN," *Wireless Commun. Mobile Comput.*, vol. 2017, Nov. 2017, Art. no. 6590713.
[66] I. You, S. Kwon, G. Choudhary, V. Sharma, and J. Seo, "An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system," *Sensors*, vol. 18, no. 6, p. 1888, Jun. 2018.
[67] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.
[68] E. Rescorla and N. Modadugu, *Datagram Transport Layer Security Version 1.2*, RFC document 6347, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6347
[69] R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P. Fernández, J. Santa, J. Hernández-Ramos, and A. Skarmeta, "Enhancing LoRaWAN security through a lightweight and authenticated key management approach," *Sensors*, vol. 18, no. 6, p. 1833, Jun. 2018.
[70] G. Selander, J. Mattsson, and F. Palombini. (2020). *Ephemeral Diffie-Hellman Over COSE (EDHOC)*. Internet Engineering Task Force, Internet-Draft draft-selander-lake-edhoc-01. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-selander-lake-edhoc-01
[71] Z. Xia, H. Zhou, K. Gu, B. Yin, Y. Zeng, and M. Xu, "Secure session key management scheme for meter-reading system based on LoRa technology," *IEEE Access*, vol. 6, pp. 75015–75024, 2018.
[72] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2011.
[73] D. Garcia-Carrillo, R. Marin-Lopez, A. Kandasamy, and A. Pelov, "A CoAP-based network access authentication service for low-power wide area networks: LO-CoAP-EAP," *Sensors*, vol. 17, no. 11, p. 2646, Nov. 2017.
[74] Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (CoAP)*, Request for Comments, IETF, RFC document 7252, Jun. 2014. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7252.txt
[75] B. Aboba, D. Simon, and P. Eronen. (2008). *Extensible Authentication Protocol (EAP) Key Management Framework*. [Online]. Available: https://tools.ietf.org/html/rfc5247
[76] D. Garcia-Carrillo and R. Marin-Lopez, "Lightweight CoAP-based bootstrapping service for the Internet of Things," *Sensors*, vol. 16, no. 3, p. 358, Mar. 2016.
[77] D. Garcia-Carrillo, R. Lopez, A. Kandasamy, and A. Pelov. (May 2017). *LoRaWAN Authentication in RADIUS, Internet Engineering Task Force, Internet-Draft Draft-Garcia-Radext-Radius-LoRaWAN-03*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-garcia-radext-radius-lorawan-03
[78] P. R. Calhoun, *Diameter Network Access Server Application*, RFC document 4005, 2005.
[79] D. Garcia-Carrillo, R. Lopez, A. Kandasamy, and A. Pelov. (May 2016). *LoRaWAN Authentication in Diameter, Internet Engineering Task Force, Internet-Draft Draft-Garcia-Dime-Diameter-LoRaWAN-00*. [Online]. Available: https://tools.ietf.org/html/draft-garcia-dime-diameter-lorawan-00
[80] I. Butun, N. Pereira, and M. Gidlund, "Analysis of LoRaWAN v1. 1 security," in *Proc. 4th ACM MobiHoc Workshop Experiences Design Implement. Smart Objects*, 2018, pp. 1–6.
[81] T. C. M. Dönmez and E. Nigussie, "Security of join procedure and its delegation in LoRaWAN v1.1," *Procedia Comput. Sci.*, vol. 134, pp. 204–211, 2018.
[82] J. Han and J. Wang, "An enhanced key management scheme for LoRaWAN," *Cryptography*, vol. 2, no. 4, p. 34, Nov. 2018.
[83] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, "Rabbit: A new high-performance stream cipher," in *Proc. Int. Workshop Fast Softw. Encryption*. Lund, Sweden: Springer, Feb. 2003, pp. 307–329.
[84] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Trusted third party based key management for enhancing LoRaWAN security," in *Proc. IEEE/ACS 14th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2017, pp. 1306–1313.
[85] R. McPherson and J. Irvine, "Secure decentralised deployment of LoRaWAN sensors," *IEEE Sensors J.*, early access, Jul. 31, 2020, doi: 10.1109/JSEN.2020.3013117.
[86] J. Kim and J. Song, "A simple and efficient replay attack prevention scheme for LoRaWAN," in *Proc. the 7th Int. Conf. Commun. Netw. Secur. (ICCNS)*, 2017, pp. 32–36.
[87] J. Kim and J. Song, "A secure Device-to-Device link establishment scheme for LoRaWAN," *IEEE Sensors J.*, vol. 18, no. 5, pp. 2153–2160, Mar. 2018.
[88] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[89] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi, and M. Rajarajan, "A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.
[90] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.
[91] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, "Enhancing key management in LoRaWAN with permissioned blockchain," *Sensors*, vol. 20, no. 11, p. 3068, May 2020.
[92] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing LoRaWAN IoT," in *Proc. 2nd Int. Conf. Crowd Sci. Eng. - ICCSE*, 2017, pp. 38–43.
[93] A. Hoeller, J. Sant'Ana, J. Markkula, K. Mikhaylov, R. Souza, and H. Alves, "Beyond 5G low-power wide-area networks: A LoRaWAN suitability study," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.
[94] 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 Commun. Mag.*, vol. 56, no. 2, pp. 60–67, Feb. 2018.
[95] 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. 103164–103180, 2020.
[96] R. K. Jha, R. S. H. Kour, and M. Kumar, "Layer based security in narrow band Internet of Things (NB-IoT)," *Comput. Netw.*, Oct. 2020, doi: 10.1016/j.comnet.2020.107592.
[97] H. Huang and L. Zhang, "Reliable and secure constellation shifting aided differential radio frequency watermark design for NB-IoT systems," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2262–2265, Dec. 2019.
[98] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," *IEEE Access*, vol. 7, pp. 114721–114730, 2019.

[99] M. Wang and Z. Qi, "A certificateless aggregate signcryption scheme without bilinear pairing," *Comput. Technol. Develop.*, vol. 27, no. 8, pp. 1–5, 2017.

[100] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. Skarmeta, "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, p. 882, Feb. 2020.

[101] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[102] D. Liu, X. Liu, H. Zhang, H. Yu, W. Wang, L. Ma, J. Chen, and D. Li, "Research on End-to-End security authentication protocol of NB-IoT for smart grid based on physical unclonable function," in *Proc. IEEE 11th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jun. 2019, pp. 239–244.

[103] Y. Lin, F. Jiang, Z. Wang, and Z. Wang, "Research on PUF-based security enhancement of narrow-band Internet of Things," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 702–709.

[104] L. Militano, A. Orsino, G. Araniti, and A. Iera, "NB-IoT for D2D-enhanced content uploading with social trustworthiness in 5G systems," *Future Internet*, vol. 9, no. 3, p. 31, 2017.

[105] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)–when social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, 2012.

[106] P. Salva-Garcia, E. Chirevella-Perez, J. B. Bernabe, J. M. Alcaraz-Calero, and Q. Wang, "Towards automatic deployment of virtual firewalls to support secure mMTC in 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 385–390.

[107] P. Salva-Garcia, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe, and A. Skarmeta, "5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks," *Secur. Commun. Netw.*, vol. 2018, pp. 1–21, Dec. 2018.

[108] R. Fujdiak, P. Blazek, K. Mikhaylov, L. Malina, P. Mlynek, J. Misurec, and V. Blazek, "On track of sigfox confidentiality with End-to-End encryption," in *Proc. 13th Int. Conf. Availability, Rel. Secur. (ARES)*, 2018, p. 19.

[109] D. J. Bernstein, "ChaCha, a variant of Salsa20," in *Proc. Workshop Rec. SASC*, vol. 8, 2008, pp. 3–5.

[110] S. M. Bellovin, "Frank miller: Inventor of the one-time pad," *Cryptologia*, vol. 35, no. 3, pp. 203–222, Jul. 2011.

[111] L. L. Moan, *ZÉRO G: Le Réseau Mondial de Connexion des Objets va Changer le Monde*, 2020.

[112] N. Haider, M. Zeeshan Baig, and M. Imran, "Artificial intelligence and machine learning in 5G network security: Opportunities, advantages, and future research trends," 2020, *arXiv:2007.04490*. [Online]. Available: http://arxiv.org/abs/2007.04490

[113] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, R. Sanchez-Iborra, and A. F. S. Gomez, "Secure bootstrapping and header compression for IoT constrained networks," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9119644/

[114] P. Thubert, A. Pelov, and S. Krishnan, "Low-power wide-area networks at the IETF," *IEEE Commun. Standards Mag.*, vol. 1, no. 1, pp. 76–79, Mar. 2017.

[115] A. Minaburo, L. Toutain, C. Gomez, and D. Barthel, *SCHC: Generic Framework for Static Context Header Compression and Fragmentation*, RFC, document 8724, Apr. 2020. [Online]. Available: https://rfc-editor.org/rfc/rfc8724.txt and https://www.rfc-editor.org/info/rfc8724

[116] A. Minaburo, L. Toutain, and R. Andreasen. (2020). *LPWAN Static Context Header Compression (SCHC) for CoAP, Internet Engineering Task Force, Internet-Draft Draft-Ietf-LPWAN-CoAP-Static-Context-HC-15*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-coap-static-context-hc-15

[117] J.-C. Zúñiga, C. Gomez, and L. Toutain. (2020). *SCHC over Sigfox LPWAN, Internet Engineering Task Force, Internet-Draft Draft-Ietf-LPWAN-SCHC-Over-Sigfox-03*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-schc-over-sigfox-03

[118] O. Gimenez and I. Petrov. (2020). *Static Context Header Compression (SCHC) over LoRaWAN, Internet Engineering Task Force, Internet-Draft Draft-Ietf-LPWAN-SCHC-Over-LoRaWAN-08*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-schc-over-lorawan-08

[119] E. Ramos and A. Minaburo. (2020). *SCHC over NB-IoT, Internet Engineering Task Force, Internet-Draft Draft-Ietf-Lpwan-Schc-Over-Nbiot-03*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-schc-over-nbiot-03

[120] M. Vučinić, G. Selander, J. Mattsson, and D. Garcia-Carillo. (2020). *Requirements for a Lightweight AKE for OSCORE, Internet Engineering Task Force, Internet-Draft Draft-Ietf-Lake-Reqs-04*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lake-reqs-04

[121] S. Delbruel, N. Small, E. Aras, J. Oostvogels, and D. Hughes, "Tackling contention through cooperation: A distributed federation in LoRaWAN space," in *Proc. Int. Conf. Embedded Wireless Syst. Netw.*, 2020, pp. 13–24.

[122] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 303–308. [Online]. Available: http://ieeexplore.ieee.org/document/8169860/

[123] J. Santa, R. Sanchez-Iborra, P. Rodriguez-Rey, L. Bernal-Escobedo, and A. Skarmeta, "LPWAN-based vehicular monitoring platform with a generic IP network interface," *Sensors*, vol. 19, no. 2, p. 264, Jan. 2019.

[124] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[125] N. Alliance, "5G white paper," Next Gener. mobile Netw., White Paper v1.0, 2015, vol. 1. [Online]. Available: https://www.ngmn.org/work-programme/5g-white-paper.html

[126] J. Mattsson, F. Palombini, and M. Vučinić. (2020). *Comparison of CoAP Security Protocols," Internet Engineering Task Force, Internet-Draft Draft-Ietf-LWIG-Security-Protocol-Comparison-04*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lwig-security-protocol-comparison-04

[127] P. Warden and D. Situnayake, *Tinyml: Machine Learning with Tensorflow Lite on Arduino and Ultra-Low-Power Microcontrollers*. Sebastopol, CA, USA: O'Reilly, 2019.

[128] R. Sanchez-Iborra and A. F. Skarmeta, "TinyML-enabled frugal smart objects: Challenges and opportunities," *IEEE Circuits Syst. Mag.*, vol. 20, no. 3, pp. 4–18, 3rd Quart., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9166461/

[129] E. Rescorla, R. Barnes, and H. Tschofenig. (2020). *Compact TLS 1.3, Internet Engineering Task Force, Internet-Draft Draft-Rescorla-TLS-CTLS-04*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-rescorla-tls-ctls-04

[130] M. Steinke, I. Adam, and W. Hommel, "Multi-Tenancy-Capable correlation of security events in 5G networks," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2018, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8725633/

[131] D. Ageyev, O. Bondarenko, W. Alfroukh, and T. Radivilova, "Provision security in SDN/NFV," in *Proc. 14th Int. Conf. Adv. Trends Radioelecrtronics, Telecommun. Comput. Eng. (TCSET)*, Feb. 2018, pp. 506–509. [Online]. Available: http://ieeexplore.ieee.org/document/8336252/

[132] A. Dhaka, A. Nandal, and R. Dixit, "Cognitive Radio Network-Based Design and Security Challenges in 5G Communication," in *Forensic Investigations and Risk Management in Mobile and Wireless Communications*. Hershey, PA, USA: IGI Global, 2020, pp. 221–241. [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-9554-0.ch009

[133] *Study on security aspects of 5G Network Slicing Management*, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) document 33.811, version 15. [Online]. Available: http://www.3gpp.org/DynaReport/33811.htm

[134] *Study on security aspects of the 5G Service Based Architecture (SBA)*, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) document 33.855, version 15. [Online]. Available: http://www.3gpp.org/DynaReport/33855.htm

[135] ETSI Technical Committee Cyber Security (CYBER), "CYBER; Application of attribute ased Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services–High level requirements, version 1.1.1," Eur. Telecommun. Standards Inst. (ETSI), Sophia Antipolis, France, Tech. Rep. TS 103 458, 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf

[136] Open Networking Foundation, "Applying SDN architecture to 5G slicing," Open Netw. Found., Palo Alto, CA, USA, Tech. Rep. TR-526, 2016. [Online]. Available: https://www.opennetworking.org/wp-content/uploads/2014/10/Applying_SDN_Architecture_to_5G_Slicing_TR-526.pdf
[137] S. Pérez, J. L. Hernández-Ramos, S. Raza, and A. Skarmeta, "Application layer key establishment for end-to-end security in IoT," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2117–2128, Mar. 2020.
[138] NIS Cooperation Group, "EU coordinated risk assessment of the cybersecurity of 5G networks," Eur. Commission, Brussels, Belgium, Tech. Rep. 62132, Oct. 2019. [Online]. Available: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf
[139] M. Lourenço, L. Marinos, and ENISA, "ENISA threat landscape for 5G networks," Eur. Union Agency Cybersecurity, Heraklion, Greece, Tech. Rep. 5G TL v1.0, Nov. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks
[140] (2020). *European Core Technologies for Future Connectivity Systems and Components (COREnect)*. [Online]. Available: https://cordis.europa.eu/project/id/956830
[141] (2020). *5G Creating Opportunities for LOGistics Supply Chain INNOVation (5G-LOGINNOV)*. [Online]. Available: https://cordis.europa.eu/project/id/957400
[142] (2020). *5G for Cooperative & Connected Automated MOBIility on X-Border Corridors (5G-MOBIX)*. [Online]. Available: https://www.5g-mobix.com/
[143] (2020). *Integrating 5G enabling technologies in a holistic service to physical layer 5G system platform (Int5Gent)*. [Online]. Available: https://cordis.europa.eu/project/id/957403
[144] (2020). *5G-DIVE: eDge Intelligence for Vertical Experimentation*. [Online]. Available: https://cordis.europa.eu/project/id/859881
[145] (2020). *A Unified Network, Computational and Storage Resource Management Framework Targeting End-to-End Performance Optimization for Secure 5G Multi-Technology and Multi-Tenancy Environments (5G-COMPLETE)*. [Online]. Available: https://cordis.europa.eu/project/id/871900
[146] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, and C. Gaber, "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, 2020, pp. 1–10.
[147] (2020). *A Cybersecurity Platform for Virtualised 5G Cyber Range Services (SPIDER)*. [Online]. Available: https://cordis.europa.eu/project/id/833685

JESUS SANCHEZ-GOMEZ received the B.Sc. degree in computer engineering and the M.Sc. degree (New Technologies) in computer science from the University of Murcia, in 2017 and 2018, respectively, where he is currently pursuing the Ph.D. degree with the Department of Information and Communication Engineering. He is also a Researcher with the Department of Information and Communication Engineering, University of Murcia, under the Fundación Séneca–Agencia de Ciencia y Tecnología de la Región de Murcia FPI Grant. His research interests include 5G, LPWANs, and the Internet of Things (IoT).

DAN GARCÍA CARRILLO received the Ph.D. degree in computer science from the University of Murcia, in 2018, under an Industrial Doctorate Grant. He is involved in the IETF in several standardization efforts regarding bootstrapping and security in the context of the Internet of Things (IoT). He is currently a Postdoctoral Researcher, continuing the research on new protocols and proposal to secure IoT in different types of constrained networks such as 6LoWPAN, 6TiSCH, LP-WAN, and, recently, 5G. He has collaborated in EU projects, such as Sociotal, SMARTIE, ANASTACIA, and Plug-N-Harvest. His main research interests are security and privacy for IoT as well as emergent technologies.

RAMON SANCHEZ-IBORRA received the B.Sc. degree in telecommunication engineering and the M.Sc. and Ph.D. degrees in information and communication technologies from the Technical University of Cartagena, in 2007, 2013, and 2016, respectively. He is currently an Assistant Professor and a Researcher with the Information and Communications Engineering Department, University of Murcia. His main research interests are evaluation of QoE in multimedia services, management of wireless mobile networks, green networking techniques, and the Internet of Things (IoT)/M2M architectures.

JOSÉ L. HERNÁNDEZ-RAMOS received the Ph.D. degree in computer science from the University of Murcia, Spain. He is currently a Scientific Project Officer with the European Commission, Joint Research Centre. His research interests include the application of security and privacy mechanisms in the Internet of Things and transport systems scenarios, including blockchain and machine learning. He has participated in different European research projects, such as SocIoTal, SMARTIE, and SerIoT. He has served as a technical program committee and chair member for different international conferences.

JORGE GRANJAL (Member, IEEE) received the Ph.D. degree in 2014. He is currently an Assistant Professor with the Department of Informatics Engineering, Faculty of Science and Technology, University of Coimbra, in Portugal. He is also a Researcher with the Laboratory of Communication and Telematics, Centre for Informatics and Systems, University of Coimbra. His main current research interests include computer networks, network security, and wireless sensor networks. He is also a member of ACM communications groups.

RAFAEL MARIN-PEREZ received the Ph.D. degree in computer science from the University of Murcia, in 2012. Since 2006, he has been with a full-time Researcher on more ten international projects, such as ARMOUR, ANASTACIA, Plug-n-Harvest, and DEMETER, as well in national projects, such as SAVIA, HospiSegur, MCiudad, and MARTA in the fields of wireless sensor networks, the Internet of Things, and cybersecurity/privacy. He is currently the Technology Manager with the Department of Research and Innovation, Odin Solutions SL.

MIGUEL A. ZAMORA-IZQUIERDO received the M.S. degree in automation and electronics and the Ph.D. degree in industrial engineering from the University of Murcia (UMU), Spain, in 1997 and 2003, respectively. In 1999, he was an Assistant Professor with the Department of Information and Communication Engineering, UMU. Temporarily, he was an External Researcher with the Laboratoire Central des Ponts et Chaussées (LCPC), Nantes, France. Since 2010, he has been an Associate Professor with the Department of Information and Communication Engineering, UMU. His research interests include ubiquitous and embedded systems, sensors fusion and integration, and communication architectures.