Secure bootstrapping and header compression for IoT constrained networks

Jesus Sanchez-Gomez
Dept. of Information and Communication Engineering
University of Murcia
Murcia, Spain
jesus.sanchez4@um.es

Dan Garcia-Carrillo
Odin Solutions SL
Murcia, Spain
dgarcia@odins.es

Rafael Marin-Perez
Odin Solutions SL
Murcia, Spain
rmarin@odins.es

Ramon Sanchez-Iborra
Dept. of Information and Communication Engineering
University of Murcia
Murcia, Spain
ramonsanchez@um.es

Antonio Fernando Skarmeta Gomez
Dept. of Information and Communication Engineering
University of Murcia
Murcia, Spain
skarmeta@um.es

***Abstract*—Security and interoperability are critical factors in Internet of Things (IoT) constrained networks in order to boost their fully integration with the Internet. In particular, secure bootstrapping and long headers compression, e.g., IPv6, are key procedures to enable end-to-end security associations with robust algorithms among cloud platforms and IoT devices. Nevertheless, few efforts are being dedicated to provide secure end-to-end authentication in IoT networks based on the prominent Low Power-Wide Area Network (LP-WAN) paradigm such as LoRaWAN. Thereby, this work discusses the security and interoperability requirements of these systems by means of a realistic use case, namely, smart-agriculture. In order to cope with the identified gaps, we present a novel solution based on the combination of the LP-WAN Static Context Header Compression (SCHC) scheme for IPv6/UDP/CoAP messages and Low-Overhead CoAP-EAP (LO-CoAP-EAP) bootstrapping. This enables the establishment of security association through IoT constrained links. Both protocols, which are two Internet Engineering Task Force (IETF) proposals, are integrated and adapted to be compliant with the LoRaWAN architecture and its stringent communication restrictions. The results show the validity of our approach with different LoRaWAN configurations, which notably increases the robustness of the overall IoT infrastructure.**

***Index Terms*—AAA, EAP, LoRaWAN, IoT, SCHC**

I. Introduction

The explosion of the Internet of Things (IoT) arrives with big challenges that still need to be addressed during the near future. One of these aspects is related to the communication technologies that provide connectivity to IoT devices or things. The arrival of the Low-Power Wide-Area Network (LP-WAN) paradigm have partially filled this gap, enabling long-range transmissions with controlled energy consumption in communication tasks. However, these notable characteristics are achieved at the expense of having available a highly constrained communication channel that only supports a reduced number of short messages per hour. This can be noticed in particular LP-WAN-based solutions such as LoRaWAN or Sigfox [1]. This fact leads to another issue in these kinds of deployments, which is the interoperability of LP-WAN systems with other IP-enabled architectures. The interconnection of heterogeneous systems is crucial to obtain end-to-end interaction between different types of devices. Given the vast number of connected IoT devices, the use of IPv6 is of relevant interest in order to have a scalable addressing space. Nevertheless, IPv6 messages are very long, which makes impossible its direct integration within LP-WAN systems.

978-1-7281-6728-2/20/$31.00 © 2020 European Union

Finally, another important challenge to be faced in LP-WAN systems is the security of the communications. Given the severe bandwidth limitations that are present in LP-WAN technologies, confidentiality and privacy methodologies that exchange packets larger than dozens of bytes are prohibitive. These devices are commonly meant to work autonomously without human supervision. While some out-of-band bootstrapping protocols are currently being standardised, they impose the need to physically reach the device. Also, confidentiality and authentication procedures of LP-WANs decrease their interoperability with other devices by being vendor-specific. Nevertheless, some technologies implement native federation and scalability options to merge already existing deployments. Still, access to third-party security domains outside of the LP-WAN back-end is not yet supported officially.

In the light of the previous discussion, in this paper we present a novel methodology that enables a bootstrapping procedure that can be employed in a wide variety of constrained devices relying in LP-WAN-based communication solutions. This bootstrapping scheme, which relies on the Static Context Header Compression (SCHC) algorithm [2] and the Low-Overhead CoAP-EAP (LO-CoAP-EAP) [3] solution, enables the integration of robust and standardized security methods within LP-WAN architectures. This permits to notably strengthen the security of deployment based on the well-known LoRaWAN technology. Thus, the main contributions of this work are: (i) an analysis of the current state-of-the-art

of authentication and key-management solutions for LP-WAN devices, (ii) a collection of the requirements from a real-life use case with regards to deployment challenges, and (iii) a methodology to perform authentication and key-management operations utilising standardised protocols over the Internet for constrained devices connected through LP-WANs.

The remaining of the paper is organized as follows. Section 2 summarises the related work about interoperability and security mechanisms in the LP-WAN ecosystem. Section 3 provides a requirement analysis by adopting a smart agriculture use-case. Section 4 presents the proposed solution and describes the main technologies integrated in the architecture as well as the interactions among the entities. Finally, the work is closed in Section 5, which also draws future research lines.

II. Related Work

The development of interoperability and security schemes in IoT scenarios is still one of the greatest issues to be solved for the realisation of large scale deployments and next-generation applications. Considering the vision of an IP-enabled IoT, the interconnection of IoT devices with limited capabilities through constrained networks demands for the use of novel mechanisms and protocols to ensure the secure and seamless information exchange among these elements. The great interest in solving this issue for LP-WAN-based solutions is evidenced by the numerous efforts done by standardisation bodies such as the Internet Engineering Task Force (IETF). Several Internet Drafts (I-D) [2], [4] and RFCs [5] documents have been released, where the use of new mechanisms for enabling IPv6-interoperability, e.g., SCHC, and the adoption of Authentication, Authorisation, and Accounting (AAA) infrastructures are envisioned as the vehicles for the development of secure and fully Internet-integrated IoT systems. Besides, the IETF security standard OSCORE [6] has been also proposed by the Open Mobile Alliance (OMA) to be integrated within LP-WAN architectures aiming at providing security at the application level [7].

Given the great success of LoRaWAN, most of the proposed solutions for achieving IPv6-enabled and secure LP-WAN systems are referred to this specific technology. For example, in [8] and [9] the performance of the SCHC compression and fragmentation scheme was explored. Both works conclude that the SCHC mechanism is a promising solution for enabling the transportation of long messages, e.g., the IPv6 ones, in LoRaWAN systems. Furthermore, a couple of IETF's I-Ds defined extensions for integrating the LoRaWAN joining procedure with AAA infrastructures such as RADIUS [10] and Diameter [11]. In this line, the work in [12] investigated the main vulnerabilities of LoRaWAN and proposed the use of the Ephemeral DiffieHellman Over COSE (EDHOC) protocol as a convenient solution for the updating process of session keys, given its low computational cost and the limited message exchanges needed. An enhanced security protocol for privacy preservation in LoRaWAN was presented in [13]. This proposal showed a very good performance in terms of end-to-end delay and message overhead although the comparison was done against different versions of the non-constrained security protocol Datagram Transport Layer Security (DTLS).

Fig. 1. Use Case of Smart Agriculture.

As an advance in comparison with previous contributions, in this work we propose a solution that consists in providing LoRaWAN deployments with IPv6 connectivity by means of the SCHC scheme and their real integration within an AAA architecture by the use of the LO-CoAP-EAP solution presented in [3].

III. Requirements Analysis in Smart Agriculture Use Case

IoT has been proven capable of providing enhanced solutions to the modernisation of smart agriculture scenarios as shown in Fig. 1. Since recently, LP-WANs allow autonomous wireless sensors and actuators monitoring and controlling agriculture fields, e.g., environment, crops, animals, etc., providing coverage to large areas with a reduced amount of base-stations. These IoT networks permit connectivity in remote regions where cellular coverage is not available, namely, 3G/4G. Moreover, IoT-based gateways permit integrating legacy equipment to interact with agriculture infrastructures for achieving information collection about environment, soil, and crops, as well as performing control actions in valves, containers, ventilation systems, pumps, etc. Data analytics permit improving complex event detection, and Decision Support Systems (DSS). Currently, there are some IoT solutions available on the market covering a range of individual operations in the agriculture sector to optimise irrigation, spraying, tree pruning, pest management, etc. However, most of these solutions are built around proprietary protocols and centralised systems with vendor dependency.

A. Key Challenges

In the next generation of smart agriculture solutions, several key challenges must be faced:

1) Interoperability of heterogeneous IoT devices and platforms from different providers. Existing devices, processing mechanisms, and DSS platforms use different protocols and technologies that heavily difficult the interactions among them. Standardised protocols are key

to enable the interoperability among components of different vendors. Smart agriculture is changing from individual solution with vendor dependency towards novel distributed and interoperable ecosystems.

2) Scalable and low-power wireless communications are critical due to the lack of power grids and wired communication infrastructure in disperse rural agricultural zones. Common Internet connectivity technologies are not available in rural areas, e.g., WiFi or cellular networks. Therefore, IoT devices require long-range low-power wireless networks and lightweight protocols to enable the communication with the application platforms deployed in the cloud.
3) Vulnerability to security and privacy threats due to distributed and spatially spread architecture formed by entities and services from multiple providers. With the increment of massive IoT device deployments and networks, more security attacks vectors are exposed. Attackers can exploit the high amount of entry-points in this complex distributed ecosystem. This specially affects farmers deploying IoT devices without specialised knowledge or tools. It is critical to provide standardised protocols to next-generation IoT services in order to make it more robust for the valuable business sector of smart agriculture.

To cope with these challenges, we propose a secure authentication and interoperable header compression based on standardisation efforts of IETF groups to enable trusted bootstrapping and end-to-end keys association of IoT devices in LoRaWAN networks to be deployed easily without specialised knowledge or tools.

IV. Background

A. LoRaWAN

LoRaWAN [14] is one of the LP-WAN-based solutions that has received greater attention from both the Academia and the Industry in recent years. This technology is supported by large companies such as Cisco or Semtech, which have joined together to give visibility to this project by means of the LoRa Alliance [15]. LoRaWAN presents a well-defined two-layered architecture: the lowest layer, LoRa, defines the physical (PHY) level, while on top of this layer, the Medium Access Control (MAC) level is defined by LoRaWAN. This technology employs unlicensed frequency bands, so its adoption has been widely generalised. This leads to a band saturation problem due to the massive number of IoT devices that will potentially coexist in highly-populated areas such as a smart city scenario. This issue is aggravated due to the low transmission-rates provided by this solution. LoRaWAN modems can configure the Data-Rate (DR) parameter, with values DR0 up to DR7, from 250 bps to 50 kbps respectively. Lower DR values are employed in adverse radio conditions to further improve signal strength, at the cost of higher energy required to transmit the data. This leads to a long time-on-air (ToA) of the transmitted packets, thus increasing the probability of collisions or interference-related problems.

Given these communication restrictions, the security scheme adopted by LoRaWAN is simple and presents some limitations. Two activation modes are defined by the specification [16]: Over-The-Air Activation (OTAA) and Activation By Personalisation (ABP). The former makes use of a pre-shared key (Application Key - AppKey), between the IoT device and the app server which is used to derive two session keys (Application Session Key - AppSKey - and Network Session Key - NwkSKey) through a *join procedure*. However, there is no defined key management or update mechanism neither for these session keys nor for the pre-shared one. Thus, an IoT device must launch the join procedure every time that session keys should be updated. In the later security scheme, ABP, both session keys must be manually installed. As can be observed, this strategy is very inflexible and introduces heavy administrative tasks for the initial configuration of the devices, therefore representing a non-practical alternative for large-scale deployments.

Therefore, the security relies on pre-provided non-removable root keys that are employed for deriving session crypto material. Those derived session keys are distributed over the LoRaWAN back-end network. The secure exchange of these keys is not specified by LoRaWAN and must be delegated to the network administrator criteria. If an attacker gains access to these keys, the data contained in the following messages transmitted over LoRaWAN get compromised. Another situation not defined by the LoRaWAN specification is how IoT devices may establish a secure association with a third-party server outside the LoRaWAN's scope.

As the adoption of more robust security schemes usually leads to the addition of extra headers and long payloads, LoRaWAN presents severe limitations to improve the strategies mentioned above. In addition, IoT devices are also highly constrained in terms of processing power and energy consumption, so they are not able to perform complex computations that are usually employed by strong security schemes. For these reasons, in the following we present a robust, low-bandwidth and computationally constrained security scheme that is able to solve the security and management issues described above. It is based on the well-know EAP scheme and makes use of the novel SCHC compression and fragmentation scheme.

B. Low-Overhead CoAP-EAP

LO-CoAP-EAP [3] is an EAP lower layer that was designed having into account the limitations of IoT scenarios, providing a lightweight bootstrapping service based on CoAP. LO-CoAP-EAP addresses the problem of the initial process of a IoT device necessary to obtain the access to data exchange in the network, i.e., the bootstrapping procedure. Bootstrapping involves a set or security operations such as authentication, authorisation and key management and it is of great importance for operators dealing with the massive numbers of IoT devices expected in LP-WAN deployments.

Current proposals to authenticate the access to IoT networks are customised to the specifications of the adopted communication technology, which leads to a problem of interoperability

when using different transmission solutions. In this sense, there is no clear effort to provide a wireless-independent network access authentication solution in IoT networks. LO-CoAP-EAP is a proposal to fill this gap for combining EAP protocol and AAA infrastructure. LO-CoAP-EAP has been tested in a LoRaFabian network [3] and in a NB-IoT infrastructure [17], in the context of LP-WAN. It also has been tested in Low-Rate Wireless Personal Area Networks (LR-WPANs) in a simulated environment , namely, Cooja, proving it is an interesting optimisation over the original design.

In this work, testing this LO-CoAP-EAP in LoRaWAN provides an advancement in the validation of the solution for different LP-WAN technologies. We also provide a further improvement over the original implementation, using the SCHC scheme for optimizing the transmission of CoAP messages.

C. SCHC

Static Context Header Compression [2] is a novel technology currently under the development of the IETF *lpwan* Work Group. It provides header compression and optional packet fragmentation, designed to be employed in LP-WAN systems. Although it has been designed in a generic manner, it is specifically tailored to IPv6/UDP packet compression. Since the IPv6 protocol inserts a relatively large overhead of 128 bits per packet, header compression achieves a significant efficiency gain for enabling LP-WAN device's access to the Internet. Additionally, a new scheme for compressing CoAP packet headers with SCHC is currently under standardisation [18]. This further improves the compression ratio of IPv6/UDP/CoAP packets.

SCHC exploits certain LP-WAN characteristics in order to perform efficient header compression. First, the star-topology of LP-WANs guarantees that the source and destination are well known in advance. Besides, embedded firmware behaviour is unlikely to change during the device's regular operation mode. Hence, the traffic flows are well known in advance by the developers. As a result, SCHC stores information about how to compress the different IPv6/UDP fields in *rules*. Each rule defines one traffic flow, and all rules are stored in a single *context*. The context is static, thus avoiding all the drawbacks from dynamic context building needed by other header compression schemes. The synchronisation signalling needed in dynamic context schemes is not present in SCHC, improving battery life and radio bandwidth usage.

Overall, SCHC's biggest contribution is hiding the architecture or interfacing details needed to communicate with devices connected to a particular LP-WAN technology. Consequently, integrating devices in existing networks becomes effortless since they are addressable through standardised Internet protocols. This is because SCHC is independent from the leveraging LP-WAN technology that delivers the packets. Yet, not all LP-WAN technologies support a maximum packet size large enough to fit the IPv6 mandatory 1280 bytes Maximum Transmission Unit (MTU). To solve this, SCHC presents an optional fragmentation procedure tailored to LP-WAN's low data rate requirements in order to comply with IPv6's MTU.

V. Proposed Solution

This section presents the proposed solution based on the integration of SCHC and LO-CoAP-EAP bootstrapping with an AAA infrastructure for LoRaWAN networks. It obtains the aforementioned improvements: (i) interoperability to authenticate against a third-party secure server through standardised protocols, and (ii) low protocol overhead that keeps the resulting messages small enough to fit LoRaWAN specifications. Fig. 2 shows the system architecture and the protocol stack.

- *IoT devices* are the furthest element of the system that will authenticate to join the security server. As a consequence, the IoT devices implement both SCHC and LO-CoAP-EAP protocols in order to communicate with the IoT controller. This proposal is aimed at constrained devices, specifically to those considered as *Class 1* and above in RFC7228. This is, devices with *System-on-Chip* microcontrollers running at 48 MHz and 32 KiB of SRAM. For instance, the *Arduino Nano* board that includes a SAMD21 MCU would fit this description.
- *Gateway* represents the LoRaWAN gateways that communicate with IoT devices through the LoRa PHY layer. No attachment procedure is performed between the IoT device and LoRaWAN gateways. Hence, gateways transparently forward all the received packets to the centralised server without inspecting their contents. These devices are geographically spread in order to give the broad coverage ranges that characterise LP-WAN technologies like LoRaWAN.
- *Network Server* (NS) and *Application Server* (AS) are part of LoRaWAN's back-end architecture. The NS is focused on managing the radio conditions and parameters of each IoT device to guarantee a robust wireless link. Also, it represents the centre of the star-topology since there is only one Network Server instance in each LoRaWAN deployment. The AS exposes a socket that behaves like a direct communication pipeline between the customer and the IoT device. In this proposal, the AS implements the SCHC adaptation layer and forwards the packets to the network. Nevertheless, the network administrator can optionally relocate the adaptation layer to an external proxy agent. Hence, no changes to the original LoRaWAN back-end software are required for our proposal to work.
- *IoT controller* is addressed by the IoT devices to perform the bootstrapping process. It decodes the LO-CoAP-EAP packets and encapsulates the data payload into a new message with the AAA protocol of choice, e.g., RADIUS or Diameter. As a result, the IoT controller forwards the EAP payload to the corresponding AAA server in charge of the EAP Authentication process.
- *AAA Server* is the end-point of the EAP authentication process. Contains the authentication credentials of each IoT device needed to perform the EAP authentication. It must support the EAP Method employed by the IoT device for the authentication process.

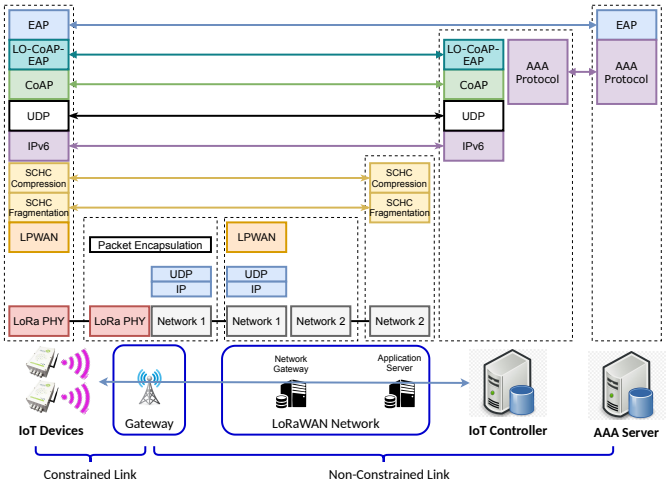

Fig. 2. Proposed architecture and protocol stack.

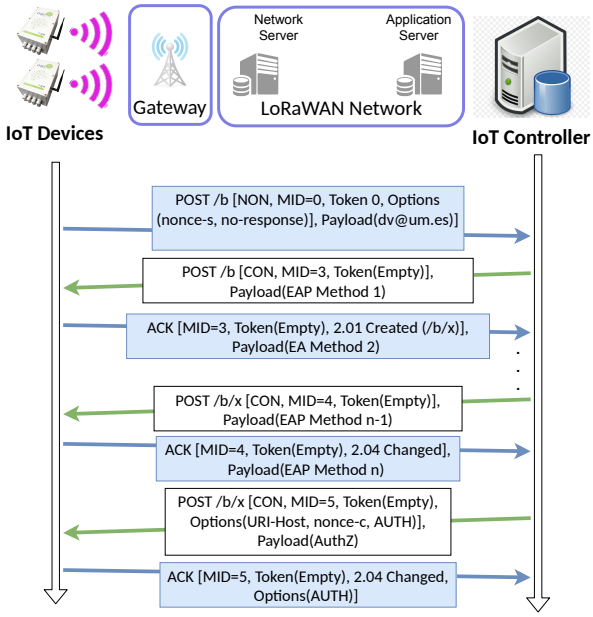

Fig. 3. Protocol message exchange diagram.

A. Interactions

Fig. 3 shows the resulting message exchange to perform authentication and key exchange by the IoT device and the IoT controller, which is described as follows. SCHC performs end-to-end compression and fragmentation tasks in order to optimise message size in the LoRa PHY constrained link. The LoRaWAN back-end guarantees that the messages reach the AS. In turn, the AS behaves like a socket abstraction of the particular IoT device by exposing an API that is seamlessly managed by the SCHC compressor/decompressor. As aforementioned, SCHC reassembles and decompresses the original message before it is being sent to the Internet. Therefore, the IoT controller does not implement any of the SCHC mechanisms or procedures. Since both ends of the LO-CoAP-EAP protocol exchange are the IoT device and IoT controller, Fig. 3 focuses on the stack above the CoAP layer. The IoT controller embeds the EAP payload into a AAA protocol, e.g., RADIUS or Diameter, to relay its contents to a AAA server. Due to the aforementioned proposal's features, the lower layers allow the delivery of messages between both authentication ends. First, the starting message in the exchange is unique in the sense that it is the only time the IoT controller acts as a CoAP client. As was noted in section IV-B, during the rest of the exchange the IoT device acts as a CoAP server instead of client. This is because CoAP servers are stateless and do not handle timers or re-transmissions. Hence, all the following steps are composed by message pairs initiated by the IoT controller instead. Additionally, the total number of messages depends on the chosen EAP Method.

TABLE I
LO-CoAP-EAP MESSAGE SIZE BEFORE AND AFTER SCHC COMPRESSION, AND MINIMUM LoRaWAN DR REQUIRED.

Packet	IPv6	Min. DR	SCHC	Min. DR
POST	71	DR3	14	DR0
POST (EAP-PSK1)	84	DR3	31	DR0
ACK (EAP-PSK2)	117	DR4	63	DR3
POST(EAP-PSK3)	116	DR4	62	DR3
ACK(EAP-PSK4)	96	DR3	45	DR0
POST(EAP-Success)	86	DR3	26	DR0
ACK	71	DR3	18	DR0

While our proposal is generic in that sense, in our case we have chosen EAP-PSK due to its relatively low computational requirements. As a result, six messages are needed to finish the process. Next, the message pair always begins with a CoAP POST targeting a certain resource `/b` first, and `/b/x` next. Furthermore, `x` is a random digit that represents the CoAP URI path of the bootstrapping process resource. The EAP messages are carried as a CoAP application payload. A CoAP *AUTH* option, which carries crypto material, is added to suit the key exchange needs. Next, the IoT device answers by piggybacking the response to the CoAP ACK packet. Also, in some instances, some crypto material is carried as part of the CoAP Options. Finally, after the last POST–ACK pair, both entities locally compute the Master Session Key (MSK). This way, the authentication and key exchange is concluded by both parties.

B. Messages size & Overhead

Table I summarises the methodology results calculated before and after compression, in terms of message size and LoRaWAN's DR value needed. The *IPv6* column shows the original message size in bytes starting with the IPv6 headers. The *SCHC* data shows the compressed message size in bytes after the SCHC procedure, i.e. the SCHC Packet length. The *Min. DR* values are the required values of LoRaWAN's DR needed to transmit the packets without any fragmentation. Table I shows a clear trend on the improvement of message length and required DR. In all instances, the messages can be transmitted in a better coverage mode, i.e., a lower DR value is attained. Given that our main aim was to reduce the bandwidth needed to perform authentication and key

exchange, the application of SCHC has proven to be a valid solution.

In order to obtain such compression ratios, the SCHC rules chosen tried to exploit the *Compression-Decompression Action Not-Sent (CDA)* or *Compute-** as much as possible. For a detailed review on the SCHC rules employed, please refer to the Appendix examples in [2], [18]. On the one hand, in the case of IPv6 and UDP compression, all the *Fields* were compressed employing *Matching Operation Equals* rules. This is attainable thanks to knowing beforehand the tuple of source and destination's IPv6 address and UDP ports. On the other hand, the selected compression rules of CoAP headers sent field values in the CoAP *AUTH* Option, the least significant 8 bits of Message ID, and the Nonce-S 32 bits. Otherwise, all the rules employed the *Not-sent* CDA.

VI. Conclusion

Secure bootstrapping is fundamental for the trusted deployment of IoT devices using LP-WAN wireless networks in decentralised scenarios such as smart agriculture and smart cities. This work proposes the combination of LO-CoAP-EAP, a lightweight bootstrapping protocol, and Static Context Header Compression (SCHC), an optimisation for the transmission of IPv6/UDP/CoAP messages in constrained networks. With this strategy the secure authentication and key management of constrained IoT devices in LP-WANs such as LoRaWAN as been enabled. The proposed solution represents the combination of two IETF's standardised efforts to reach highly flexible and scalable bootstrapping procedure over the Internet. Furthermore, the paper discussed how constrained IoT devices connected to a LoRaWAN network are able to employ the methodology to bootstrap and establish keys from a AAA infrastructure. In particular, the proposal enables to derive keys between constrained IoT devices and the IoT controller deployed in the cloud for allowing secure channels that protect data' confidentiality and privacy. The presented results have proven the validity of the solution in terms of the reduced length obtained for the messages employed during the bootstrapping procedure, which makes this process suitable to be adopted by LP-WANs. Future real experiments with multiple IoT devices configurations and energy consumption analysis will be performed in order to validate our approach and provide further improvements.

VII. Acknowledgments

This work has been partially funded by the EU H2020 projects: Plug-n-Harvest with GA 768735, Fed4IoT with GA 814918, CYSEMA with GA 777455, and IoTCrawler with GA 779852. Moreover, the paper has been also supported by Spanish Administration projects and grants, namely, FPI Grant 20751/FPI/18 of Seneca Foundation in Murcia Region, THD GUARDIAN with GA TSI-100110-2019-20 as well as Grant DI-16-08432 for Industrial Doctorate from MINECO and PEANA UNMU13-2E-2536.

References

[1] R. Sanchez-Iborra and M.-D. Cano, "State of the art in lp-wan solutions for industrial iot services," *Sensors*, vol. 16, no. 5, 2016.

[2] A. Minaburo, L. Toutain, and C. Gomez, "LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP," Internet Draft, Internet Engineering Task Force, 2019. [Online]. Available: https://tools.ietf.org/html/draft-ietf-lpwan-ipv6-static-context-hc-24

[3] 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. [Online]. Available: http://www.mdpi.com/1424-8220/17/11/2646

[4] A. Minaburo, L. Toutain, C. Gomez, J. Paradells, and J. Crowcroft, "LPWAN Survey and GAP Analysis," Internet Draft, Internet Engineering Task Force, Oct. 2016. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-minaburo-lpwan-gap-analysis-02

[5] S. Farrell, "RFC8376: Low-Power Wide Area Network (LPWAN) Overview," RFC, Internet Engineering Task Force, May 2018. [Online]. Available: https://tools.ietf.org/rfc/rfc8376.txt

[6] G. Selander, J. Mattsson, F. Palombini, and L. Seitz, "RFC8613: Object Security for Constrained RESTful Environments (OSCORE)," RFC, Internet Engineering Task Force, 2019. [Online]. Available: https://tools.ietf.org/rfc/rfc8613.txt

[7] Open Mobile Alliance, "Lightweight machine to machine requirements (White Paper)," Tech. Rep., 2013. [Online]. Available: http://www.openmobilealliance.org/release/LightweightM2M/V1_0-20141126-C/OMARD-LightweightM2M-V1_0-20131210-C.pdf

[8] C. Gomez, A. Minaburo, L. Toutain, D. Barthel, and J. C. Zuniga, "IPv6 over LPWANs: Connecting Low Power Wide Area Networks to the Internet (of Things)," *IEEE Wireless Communications*, pp. 1–8, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8994201/

[9] J. Sanchez-Gomez, J. Gallego-Madrid, R. Sanchez-Iborra, J. Santa, and A. F. Skarmeta Gómez, "Impact of SCHC Compression and Fragmentation in LPWAN: A Case Study with LoRaWAN," *Sensors*, vol. 20, no. 1, p. 280, jan 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/1/280

[10] D. Garcia-Carrillo, R. Lopez, A. Kandasamy, and A. Pelov, "LoRaWAN Authentication in RADIUS," Internet Draft, Internet Engineering Task Force, May 2017. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-garcia-radext-radius-lorawan-03

[11] D. Garcia-Carrillo, R. Lopez, A. Kandasamy and A. Pelov, "LoRaWAN Authentication in Diameter," Internet Draft, Internet Engineering Task Force, May 2016. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-garcia-dime-diameter-lorawan-00

[12] R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P. J. Fernández, J. Santa, J. L. 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. [Online]. Available: http://www.mdpi.com/1424-8220/18/6/1833

[13] 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. [Online]. Available: http://www.mdpi.com/1424-8220/18/6/1888

[14] "A technical overview of LoRa and LoRaWAN," LoRa-Alliance, Tech. Rep., 2015.

[15] "LoRa-Alliance," https://www.lora-alliance.org/. [Online]. Available: https://www.lora-alliance.org/

[16] LoRa Alliance, "Lorawan specification version 1.0," *LoRa Alliance*, 2015.

[17] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. F. Skarmeta, "Secure Authentication and Credential Establishment in Narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, p. 882, feb 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/3/882

[18] A. Minaburo and L. Toutain, "LPWAN Static Context Header Compression (SCHC) for CoAP," Internet Draft, Internet Engineering Task Force, Dec. 2019. [Online]. Available: https://tools.ietf.org/html/draft-ietf-lpwan-coap-static-context-hc-12