Journal of Engineering and Applied Sciences 14 (24): 9774-9787, 2019
ISSN: 1816-949X

Internet of Things: A Security Survey Review on Long Range Wide Area Network (LoRaWAN)

[1, 2]Jhonattan J. Barriga A. and [1, 2]Sang Guun Yoo
[1]Facultad de Ingenieria en Sistemas, Escuela Politécnica Nacional, Quito, Ecuador
[2]Smart Lab, Escuela Politécnica Nacional, Quito, Ecuador
jhonattan.barriga@epn.edu.ec, sang.yoo@epn.edu.ec

Abstract: The exponential growth of Internet of Things (IoT) is bringing new technologies, protocols and devices that demands long range connections. And for covering this needs, new technologies such as Low Power Wide Area Networks (LPWAN) have emerged. One of the most popular LPWAN technologies is Long Range Wide Area Network (LoRaWAN) which aim to provide long range connections using low amount of energy. This technology is very useful for delivering several types of data such as temperature, humidity, water consumption and home security data, among others. However, since, LoRaWAN simplifies data packets and provides reduced security features to preserve energy, IoT devices using such technology have been severely compromised in the past. LoRaWAN has addressed some security issues found in the past but as every technology that is gaining adepts, it has been threated continuously through different types of attacks. This study aims to perform a systematic review process to examine the state of security of this protocol by analyzing discovered vulnerabilities and proposed countermeasures.

Key words: LoRaWAN, mitigation mechanisms, security, threats, vulnerabilities, proposed countermeasures

INTRODUCTION

The world of Internet of Things (IoT) is growing, exponentially, in such a way that by 2020, there will be nearly 20 billion devices connected to internet (GI., 2015). Likewise, several types of protocols have been proposed to support connectivity to IoT devices and one of the most important is the Low Power Wide Area Networks (LPWAN) protocols. LPWAN protocols have several benefits such as low power consumption, low cost sensors and wide coverage; however, they also have disadvantages such as low bandwidth operation (Kuo *et al*., 2017). The most popular LPWAN protocols are LoRa, LoRaWAN, SigFox and NB-IoT (Mekki *et al*., 2019). Main applications of these protocols are temperature sensing, smart parking, water meter, smart garbage cans among others.

LoRaWAN is a network protocol based on LoRa physical specification, developed by LoRa-alliance (Kuo *et al*., 2017). It means long range wide area network protocol and it is quite new protocol which first specification was released in 2015, the last specification i.e., 1.1 was recently published in October 2017. LoRaWAN is oriented to optimize battery lifetime, delivery long range and reduce costs. Its scheme is mainly composed of end-devices, gateways, network servers and application servers (LA., 2017). In terms of security, its major remark is that it uses data encryption using session keys based on symmetric cryptography.

The appearance of new technologies such as LoRaWAN opens the door for new development opportunities but they also create new threats and vulnerabilities which could compromise not only devices but also information of end-users. Although, LoRaWAN considers some security features in its implementation, several vulnerabilities have been found in previous versions which were addressed in the new specification, however, new threats have risen even security improvements (Butun *et al*., 2018).

This study aims to review and discuss LoRaWAN security features and vulnerabilities discovered in the past by developing a systematic review to depict the current state of security of LoRaWAN.

MATERIALS AND METHODS

The main objective of this research is to analyze the security features and vulnerabilities present in LoRaWAN protocol. Therefore, a research method will be applied to achieve such goal. The research method that have been

Corresponding Author: Sang Guun Yoo, Facultad de Ingenieria en Sistemas, Escuela Politécnica Nacional, Quito, Ecuador, sang.yoo@epn.edu.ec

used to carry out the present review research consisted of three major phases: plan, perform review and report (Fig. 1) as suggested by Kusen and Strembeck (2017).

Plan phase: This phase is the initial setup before starting a research. It allows to narrow the scope and produce proper findings. In this phase, definition of research questions was executed as the first step. In this case, two research questions have been considered:

- What are the security features present in LoRaWAN protocol?
- What are the security vulnerabilities, attacks or threats that might compromise the Confidentiality, Integrity and Availability (CIA) in LoRaWAN deployments?

Based on the research questions, the next step was to identify keywords. The identified keywords were: lorawan, security, vulnerabilities and threats. Keywords were used to build search strings that were the input for research databases. These search strings might contain combinations of keywords and logic operators such as "AND", "OR", "NOT". Such combinations were later refined to search for papers that were related to the subject of study and were the input for the next step called "define databases". The purpose of defining databases was to identify searchable repositories that contain in-formation related to the review and from where papers will be retrieved. For this purpose, four main databases have been selected: ACM Digital Library, Science Direct, Springer Link and IEEE Xplore Digital Library. In summary, this phase was composed of three steps: define research questions, define search strings and define databases (Fig. 2).

Fig. 1: Research method used in this study

Perform review phase: This phase includes the search of articles in different databases and discarding of those papers that are not related to the subject of study. This phase will deliver a small set of papers that comply with all the criterion defined before which will be used as an input of the present review study. A summary of the steps followed is displayed in Fig. 3.

To perform the review, different search strings were built and applied to the selected databases. Every query produced a set of results that were later exported as a bibtex list file for ACM, Science Direct and IEEE Xplore. For Springer Link, a CSV containing all the results was obtained; then by opening the CSV, we extracted the DOI and with the help of Zotero ("Zotero|Downloads," n.d. Anonymous, 2018), we obtained a dataset containing details of every article and then results were exported to a bibtex list file.

Then, all the BibTex file lists were consolidated into one and imported into Mendeley ("Mendeley-Reference Management Software & amp; Researcher Network," n.d.). Every entry from the consolidated file represents an article and every article contains attributes that will be reviewed to select candidate papers mainly title, year and abstract. Mendeley was mainly used to take notes on papers that comply with the proposed research questions.

During this phase the following amount of papers were found by using different search strings (Table 1 and 2). In the first stage of search, 870 papers were found, however, after removing duplicate entries with the help of Mendeley, it ended up into 376 relevant papers to the

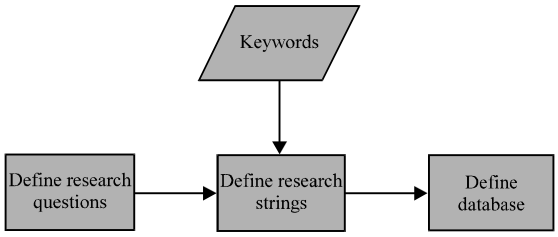

Fig. 2: Plan phase

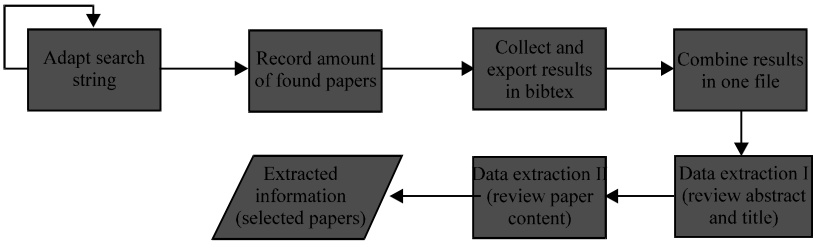

Fig. 3: Perform review phase

Table 1: Science direct and springer link query results

Science direct		Springer link	
Search strings	Results	Search strings	Results
LoRaWAN threats	0	LoRaWAN threats	0
LoRaWAN vulnerabilities	0	LoRaWAN security	0
LoRaWAN security issues	0	LoRaWAN vulnerabilities	0
LoRaWAN security	2	LoRaWAN security issues	0
LoRaWAN threats	18	LoRaWAN vulnerabilities	10
LoRaWAN vulnerabilities	21	LoRaWAN threats	11
LoRaWAN security issues	41	LoRaWAN security issues	49
LoRaWAN security	44	LoRaWAN security	64

Table 2: ACM digital library and IEEE xplore digital library query results

ACM digital library		IEEE xplore digital library	
Search strings	Results	Search strings	Results
LoRaWAN threats	0	LoRaWAN threats	0
LoRaWAN security issues	0	LoRaWAN vulnerabilities	0
(+LoRaWAN+threats)	1	LoRaWAN security issues	0
LoRaWAN vulnerabilities	1	LoRaWAN security issues	1
LoRaWAN security	2	LoRaWAN threats	3
(+LoRaWAN+security+ issues)	2	LoRaWAN security	3
(+LoRaWAN+ vulnerabilities)	3	LoRaWAN vulnerabilities	8
(+LoRaWAN+security)	9	LoRaWAN security	30
		((LoRaWAN) and vulnerabilities)	51
		((LoRaWAN) and threats)	65
		(((LoRaWAN) and security) and issues)	177
		((LoRaWAN) and security)	254

research questions. Papers beyond August, 2018 were discarded as they have not been published yet. No papers were discarded for being old, since, the oldest was from 2015. Journals and proceedings in English language were considered in the search phase.

Moreover, to identify papers to be analyzed in depth, a brief review of the title and abstract was performed, searching for articles that address LoRaWAN security features, vulnerabilities and threats. At the end this process, 72 papers remained for further review. From this set, 37 papers were related to the subject of study; the other 35 were used to support and document LoRaWAN features. Finally, a last review was performed to discard duplicate or inadequate papers. A total of 31 papers were selected to write this security compilation of LoRaWAN.

Reporting phase: This is the last phase of our proposed and adapted research method. During this last stage all findings and results were documented and discussed. It is important to consider that during this phase some refinement was done because remaining papers needed to be reviewed in depth to validate research pertinence compliance. In the next section, a depth discussion and review of the selected papers that expose vulnerabilities of LoRaWAN specification 1.1 was executed.

LoRaWAN: LoRaWAN which stands for Low Power Wide Area Networks (LPWAN) (Butun *et al*., 2018; Anonymous, 2018a) includes several interesting features such as long-range communication, low energy consumption and secure data transmission. LoRaWAN protocol uses unlicensed radio spectrum in the Industrial, Scientific and Medic (ISM) bands (Semtech.com, n.d.) (LA., 2017) and it is currently based on the specification Version 1.1 released in October 2017 (LA., 2017).

Network deployment architecture: LoRaWAN architecture is composed by four main elements. First, IoT end node devices oversee collecting information from several sources within an application environment e.g., water meter, light bulbs and vehicle tracking. Such devices are connected to special devices called gateways using the LoRaWAN protocol. Then, LoRa gateways transform LoRaWAN frames into IP packets and connect to network servers. Finally, data arrives to application servers where it is processed accordingly to business needs (Kuo *et al*., 2017) (Fig. 4).

The current release of LoRaWAN adds extra roles for network servers, mainly to work in roaming environment. Those roles are: home Network Server (hNS), serving Network Server (sNS) and forwarding Network Server (fNS). Likewise, application server has been divided in two additional roles that are: Join Server (JS) and Application Server (AS). These new features aim to provide roaming capabilities for backward support (LoRaWAN 1.0) as well as increasing security. In regards of the overall architecture, there are no major changes among the protocols used to perform connections.

Security features: One of the most remarkable properties of LoRaWAN is that it uses symmetric encryption based on AES-128 to guarantee end-to-end security. To handle encryption, end-node devices are preloaded with a pair of root keys known as Appkey and NwkKey which are unique for each device. These keys are used to derive two lifetime keys JSIntKey and JSEncKey, three network session keys NetSKeys (SNwkSIntKey, FNwkSIntKey, NwkSEncKey) and one application session key AppSKey. Integrity and confidentiality are main features of those keys as they protect join-request messages and join-accept messages triggered by join-request messages (LA., 2017).

To guarantee integrity and authenticity, a cryptographic Message Integrity Code (MIC) is generated. This MIC is calculated as shown in Eq. 1 and 2. Likewise, Fig. 5 shows the place of MIC. It is placed at the end of MAC pay-loads:

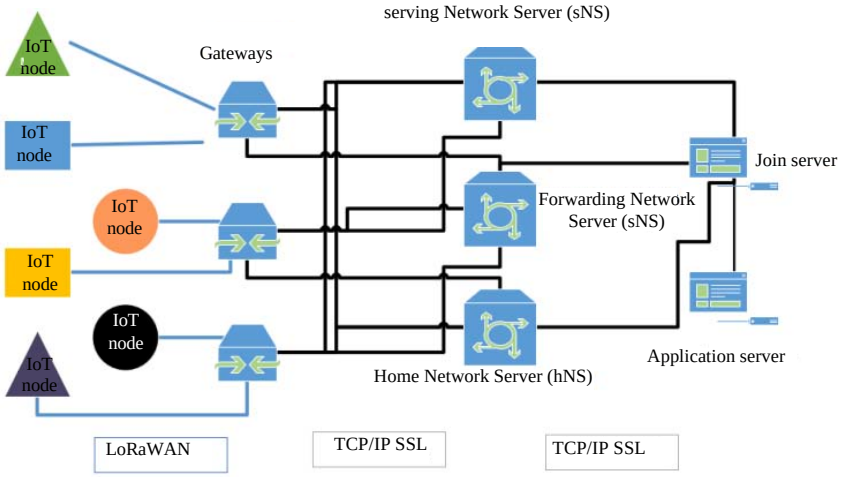

Fig. 4: LoRaWAN network architecture

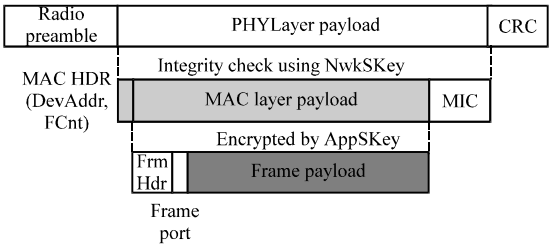

Fig. 5: MIC with MAC header and payload (Yang *et al*., 2018)

$$cmac = aes128\_cmac(NwkKey, MHDR|JoinNonce|NetID|DevAddr|DLSeetings|RxDelay|CFList) \quad (1)$$

$$MIC = cmac[0..3] \quad (2)$$

In regards of end-node activation, there are two processes known as Over The Air Activation (OTAA) and Activation by Personalization (ABP). These processes look forward to securely attach a valid node to the LoRaWAN network. In ABP DevAddr, FNwkSIntKey, SNwkSIntKey, NwkSEncKey and AppSKey are directly stored in the end node device instead of being derived from the DevEUI, JoinEUI, AppKey and NwkKey during the join procedure (LA., 2017). Whilst in OTAA the end-node has to be personalized with DevEUI, JoinEUI, AppKey and NwkKey before the join procedure. During OTAA activation scenario, network session keys are derived to encrypt and transmit at the network level. The OTAA activation procedure is explained in Fig. 6.

Vulnerabilities and mitigation mechanisms: There are several works discussing LoRaWAN vulnerabilities and possible countermeasures. One of them found and exploited five potential vulnerabilities for specification 1.0.2 (Yang *et al*., 2018). The identified vulnerabilities were: replay attack for ABP-activated nodes, an attacker might use older messages and resend during the current session leading to a lost communication between node and network server, eavesdropping as the key is reused on every cipher text, an attacker might be able to decrypt information based on previous messages sent with the same key, bit-flipping attack, although, information is encrypted, it could be messed up. In this case, through a MITM between TCP connections, an attacker might modify certain bytes of the encrypted payload, ACK Spoofing, previously captured ACK could be delayed to selectively acknowledge the successful receipt of another distinct message, even, if it has not arrived yet to the backend provider, LoRa class B attacks, a malicious user might attempt to drain the battery of the device by modifying beacon payloads as they are not encrypted. The aforementioned vulnerabilities show weaknesses over LoRaWAN that affect integrity, availability and confidentiality. Probably, the most critical is the one that affects integrity in spite of having a secure symmetric algorithm in place (AES-128), attackers are able to modify information. Anyhow, the vulnerabilities described before have apparently been solved in LoRaWAN according to an analysis performed by Donmez and Nigussie (2018).

Kim *et al*. propose a dual key based schema for a secure authentication in LoRaWAN 1.0.2 (Kim and Song, 2017b). The researchers analyze security problems during end-node activation over OTAA. In this approach, they propose the inclusion of a new key called NwkKey. It has to be stored in the end-node and must not be shared with others. Such key is pre-shared only with NS

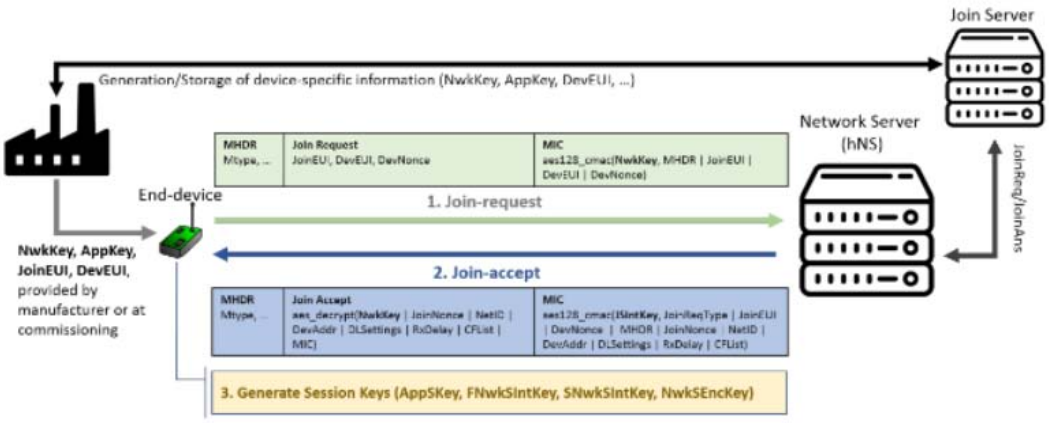

Fig. 6: LoRaWAN OTAA activation procedure (Butun *et al*., 2018)

and will be used to to generate a new session key called as (NwkSKey). On the other hand, the preexisting AppKey is pre-shared only with AS. With this approach, the OTAA procedure changes a bit as described by the researchers. The researchers have proposed several previous steps that are performed before establishing a communication. First of all, the initial join request is generated and sent to the NS with the NwkKey instead of the AppKey. Then, as the NS knows the NwkKey, it will calculate the MIC again to validate the join request. If such validation is successful the NwkSKey will be generated. Later, AS generates the AppSKey based on the AppKey previously shared. Then, the AS sends the AppNonce to the NS. Furthermore, the NS sends the join accept message which contains NwkNonce and AppNonce encrypted with NwkKey and AppKey respectively. Finally, the end-node decrypts the join accept message and generates NwkSkey and AppSKey which are going to be used instead of the previous pre-shared keys to prevent a key-leakage. The inclusion of this new key aims to delegate authentication to every server in the architecture. This proposal has 1 been remarkable, as this new key was included in the new specification of LoRaWAN 1.1. Also, the inclusion of this new key provided backward compatibility scenarios when dealing with devices working on Versions 1.0.2 and 1.1 as described in LoRaWAN 1.1 specification (LA., 2017).

Several vulnerabilities have been identified in LoRaWAN as part of an analysis of the LoRaWAN 1.1 specification (Butun *et al*., 2018). In this review, the researchers highlight six attacks. First, the researchers indicate that RF jamming attack affects gateway and end-node letting attackers to jam such traffic. Moreover, they explain that replay attacks affect the join procedure where an attacker can jam signals for the OTAA session; an attacker might use previous join-request to connect to the network server. Besides, the aforementioned work indicated that beacon synchronization attack might let malicious users to set up gateways sending fake beacons. In addition, network traffic analysis would be exploited by an attacker that sets a rogue gateway to capture information. Additionally, it also warns that by executing a man-in-the-middle attacks against servers, might compromise unencrypted communication between network server and application server which means that this vulnerability is still present in the new specification of the protocol. Finally, the researchers use a tool called Scyther to assess cryptography over LoRaWAN where they indeed have concluded that it is a strength point of the protocol. From the vulnerabilities described before, the first three lead to a DoS attack and the rest are related to traffic analysis and MITM attacks (Butun *et al*., 2018).

Replay attacks have been addressed and discussed in depth for LoRaWAN Version 1.0.2 as in (Iskhakov *et al*., 2017; Kim and Song, 2017a; Na *et al*., 2017; Sung *et al*., 2018; Tomasin *et al*., 2017). One of the proposed solutions aims to identify moving nodes and try to differentiate malicious nodes from valid nodes. This solution is oriented to support join procedure over the network server. The researchers address this attack by using Received Signal Strength Indicator (RSSI) which are used to measure the strength of signal and propietary hand-shaking. In this scenario, the researchers propose that the RSSI should be stored along with the DevNonce to compare it with future requests and validate that are not repeated. Validating the RSSI just by itself is not enough and therefore, the server must send a proprietary message (MType set to 111) instead of join-accept for the join request. The end-node device responds to the

proprietary message of network server with the same MType. This proprietary message is encrypted, so that, it could not be modified by an attacker. Anyhow, researchers recommend that it is necessary to validate users through RSSI rather than generating proprietary messages for every join requests (Sung *et al*., 2018). Another proposal is described by Kim and Song (2017a) where the researchers work on LoRaWAN Version 1.0.2 to build a mitigation scenario. The proposed scheme redefines the initial and non-initial join request. Non-initial join request is used in standard conditions and helps to confirm the validity of NwkSKey to prevent replay attacks. Whilst, initial join request is used when the NwkSKey does not exist in the node and prevents replay attack using the DevNonce. This initial join request is valid no matter, if the NwkSKey is lost on the end node (Kim and Song, 2017a).

Join Request in Over The Air Activation (OTAA) was the scenario that Na *et al*. (2017) used to identify a replay attack and later propose a solution. The researchers manifest that join requests are sent in plain text; therefore, an attacker might sniff join-requests from other devices and then try to resend them to the network server. If it responds to those old join-requests any valid node will not be able to communicate. To address this problem, they suggest to use a token that could be XORed with the current join request. This token indeed is a previous NwkSKey which will allow to mask the current request (Na *et al*., 2017).

Another work is the development of the security analysis of LoRaWAN join procedure for internet of things networks (Tomasin *et al*., 2017). The researchers have identified that it is not necessary for an attacker to be present in order to compromise the network, as there is a chance that an end-device could generate a previous DevNonce. They perform experimentation over a SX1272 modem by using a jammer and measured the entropy level. They concluded that the proximity reduces entropy level of the end-device, affecting its ability to produce random information (Tomasin *et al*., 2017).

By Iskhakov *et al*. (2017) an analysis of vulnerabilities in low-power wide-area networks is performed over LoRaWAN 1.0.2. This research depicts two main vulnerabilities. First, replay attacks during any type of end-node activation mechanism (ABP or OTAA) during join procedure. Under this scenario an attacker could send previous join-accept or join-request to disable an end-devices. The second vulnerability identified was ACK spoofing. In this case, an attacker could intercept and resend the same ACK message to confirm various messages from the end device. For this scenario, the attacker must have compromised the gateway before. In this research, researchers have not performed an experimental procedure but support their findings on reviewing and analyzing the LoRaWAN specification (Iskhakov *et al*., 2017).

In 2016, a secure architecture was proposed (Naoui *et al*., 2016). The approach was to include a Certification Authority (CA) at the gateway level to use it for authentication handling, authorization and key management of nodes. This solution contemplates the use of tables to identify certificates of nodes, a trust table to identify the level of trust of a particular gateway and a black list of nodes. A strength of this solution is that it considers a de-authentication phase and the possibility of changing the CA. In this scenario, a MITM is not possible as messages are cyphered with public keys.

Aras *et al*. (2017a, b) in their research, identified vulnerabilities in LoRaWAN 1.0.2 specification. The vulnerabilities found have to do with compromising devices and network keys, assuming that a malicious attacker might have physically accessed the device and was able to extract root keys by using Xignal mousetrap. Also, jamming techniques were possible by using cheap devices to flood LoRa channel causing communication unavailability (Aras *et al*., 2017a, b). Besides, replay attacks over ABP join procedures and wormhole attacks are possible when an attacker captures packets from one device and resends them to a distant device to replay a hijacked packet (Aras *et al*., 2017a, b). To prevent jamming attacks, an initiative based on a network intrusion detection system is discussed by Danish *et al*. (2018); this approach is based on analysis of two algorithms i.e., Kullback Leibler Divergence (KLD) and Hamming Distance (HD). At the end, the researchers found out that KLD performs better and it would be useful to detect jammers within the radio of a LoRaWAN end node.

Although, LoRa alliance has developed a new specification for LoRaWAN in order to address previous vulnerabilities, there might still be security issues and this situation is discussed by Donmez and Nigussie (2018). In regards of join procedure, the researcher identifies four main threats i.e., key management, join procedure delegation, backward compatibility and replay protection in join procedure. LoRaWAN 1.1 specification includes a handover roaming which opens the threat for a Man-in-The-Middle attack (MITM), since, FRMPayloads are first transported from the serving Network Server (sNS) to the home Network Server (hNS) and then to the Application Server (AS). LoRaWAN specification does not reinforce physical tampering protection. Indeed, it increases the possibility of compromising root keys as a malicious user with physical access to device might steal them to decrypt information.

The mechanism proposed in this research would address this issue as root keys will only be used to perform an initial joint procedure and then deleted from the node. In the eventual scenario of an attacker compromising the node, it will not be possible to discover previous session keys. Hence, to properly address key leakages, it is mandatory that the NS records previous AppSKey (Kim and Song, 2017b). To support backward compatibility, a new root key (NwkKey) is used to handle join request delegation. But if there is no proper forward secrecy when the new root key is taken by an attacker, data from end-node might be exposed and decrypted. This research contributes with two alternatives to address the threat, first the researcher indicates that the node should be configured to always derive AppSKey based on AppKey no matter the value of OptNeg he also explains that it is necessary to set the version of the protocol in the node. The researcher also indicates that a malicious NS might be able to replay OTAA activation messages on the join server compromising integrity and confidentiality of application data as there might be an overflow of counter nonce. For this scenario, the researcher proposes that the Join Server (JS) must record previous DevNonce and Jcount0 last values, giving the possibility that JS would be able to identify a possible overflow of JoinNonce and stop receiving requests from a particular node. These suggestions are based on protocol review rather than experimentation.

Denial of Service (DoS) also affects LoRaWAN 1.1 as described and tested by Van Es *et al.* (2018). The researchers used Coloured Petri Nets (CPNs) and with the help of CPN-tools, they simulated and analyzed the following vulnerabilities that could result in a DoS attack. First, beaconing is a vulnerability that has to do with class-B beacons broadcasted by gateways to schedule reception windows. These beacons are not encrypted or signed. In these circumstances, an attacker might be able to modify timing references, producing a desynchronization of the window reception, leaving the node unable to communicate with the network server. According to the researcher and supported by Miller (2016) this vulnerability is still present in LoRaWAN 1.1. Another vulnerability is downlink routing. First of all, anytime the network wants to start a downlink traffic to a node, it has to rely on the gateway that is aware of a previous uplink transmission. During the uplink procedure, nodes broadcast their data to the nearest gateways and then forward packets to the NS (which is able to track previous gateways used by a particular node). However, an attacker can eavesdrop uplink transmission and respond through a gateway that is out-of-reach of the end-node, causing that a valid gateway near from a node would be discarded as it has been unauthenticated by the malicious gateway. This vulnerability was discovered in Version 1.0 and according to the researchers it is still present in the new specification. The last vulnerability found in this research is known as join-accept replay vulnerability. In ABP, network server provides configuration settings and those have to be inserted manually in the end-node. Meanwhile, OTAA is more pliable as with few configurations in the node, it will be able to exchange information with the NS and synchronize configuration details. The weakness is that there is no reference in the except for a previous request. According to Van Es (2018), this vulnerability has been addressed for Version 1.1 but since, there is a compatibility for devices running Version 1.0.2, the vulnerability is still present for such devices in the new specification. This research is the latest in regards of vulnerabilities associated to LoRaWAN 1.1.

A report from the industry written by R. Miller from MWR Labs (Miller, 2016), identifies seven vulnerabilities in LoRaWAN 1.0 solutions. First of all, weaknesses in key management as AppKey is stored in two places (end-nodes and servers). In regards of key usage, if the message payload is analyzed before considering the MIC field, an attacker might bit-flip the information to modify its content. Second, weaknesses in key generation if keys used over ABP are generated over a simple procedure such as using device address, an attacker might reverse it to find out the way to compromise all other nodes. Third, devices are supposed to be trusted; however, the information generated by them could have been mangled. For instance, it might include bogus characters that would allow an attacker to execute a SQL Injection attack. Moreover, the gateway could be compromised as it has internet connectivity and if it has not been properly hardened, it could be compromised. This vulnerability is present over all devices with an IP connection to the internet in such case a VPN would help to reduce the risk of exposure. In addition, an invalid counter control would lead an attacker to devise a payload; therefore, a proper control should be in place to reduce the risk. Finally, in terms beacons and multicast messages there is no way for the node to know that they were generated by an authentic entity of the system. This research shows a brief enumeration of the vulnerabilities present and described in other works but do not make a further analysis of them and suggest brief recommendations for preventing such attacks. Vulnerabilities described in this reseach have also been listed and discussed by Na *et al.* (2017).

One of the most common issues in regards of LoRaWAN V1.0.2 is the key management process as

revised by Sanchez-Iborra *et al*. (2018). The researchers denote that a major concern of this protocol is key sharing. During the OTAA procedure the shared AppKey is used to derive NwkSKey and AppSkey. This procedure is perfomed the first time a device connects to the network. However, during ABP both keys (NwkSKey and AppSkey) must be written in the device, making this a notable insecure procedure as those keys are never updated. Considering the ABP scenario those static session keys have a great rate of being compromised due to their lack of dynamicity. An attacker obtaining those keys would be able to decrypt all the information being sent. On the other hand, in LoRaWAN 1.1 some security measures have been considered to improve the generation of session keys; however, the procedure is still insecure as the generation of new session keys is based on two non-removable keys (AppKey and NwkKey) that have been previously loaded inside the end-device. To mitigate this vulnerability, researchers propose the inclusion of EDHOC which is a lightweight key exchange protocol for establishing symmetric keys among two end-node devices. To integrate this solution to the current LoRaWAN protocol, researchers have designed three messages to securely update session keys. This protocol will be acting between the end-node and the network server according to the researchers. EDHOC acts on top of other protocols and will be able to derive NwkSKey and AppSKey previously obtained through OTAA. It is important to consider that before any communication an EDHOC negotiation must be executed to derive the previous mentioned session keys. Researchers have shown that this solution will not use more than 176 bytes which can be supported by the greatest data-rate of LoRa configurations known as SF7 and SF8. The solution discussed before has been tested over LoRaWAN V1.0.2 and it might need to be modified to be supported by current version of LoRaWAN protocol 1.1.

Five types of attacks have been identified, discussed and analyzed by Avoine and Ferreira (2018). The research was merely focused on LoRaWAN Version 1.0. It shows weak points of the protocol in regards of decrypt attacks and DoS attacks. First of all, a device might be forced to reuse previous session keys making it possible that a frame of a past session would become valid and hence, replayed to the Network Server (NS). To execute this attack, a device must use a repeated DevAddr, DevNonce and AppNonce. The researchers support their statement on the birthday paradox and hence, if an attacker is able to compromise the AppNonce (3-bytes length), the randomness of the session will only depend on DevNonce (2-byte length) parameter. Likewise, the specification does not clearly state how to handle unconfirmed join requests. In this scenario, a join request might contain a previously generated DevNonce. A replay attack is possible with the previous scenario because frames from previous sessions might be replayed in a new session. A message decryption is feasible through the described scenario as the device uses the same keystream to protect different frames. According to the researchers a similar approach can be directed to target the NS making it to use the same DevAddr, DevNonce and AppNonce without performing any validation as the specification states that a record of some DevNonce must be stored. Therefore, if the attacker is able to force the server to generate the same security parameters, a replay attack might be executed. This attack is possible as the AppNonce is not long enough and it is pseudo-generated. On the other hand, denial of service attacks could affect end-node devices and NS. The main objective of this attack is to disconnect the device form the network by forcing it not to share its new session keys with the NS. The lack of confirmation of a join accept with a corresponding join request makes the device to be out of the network. Similarly, if the NS completes the key exchange procedure with the device all messages sent to the device will be ignored. AppNonces are generated every time a join request is received but if an attacker is able to replay to the NS with a previous join request the end-node device will not share the same session keys. The researchers point out that a lack of integrity between the NS and the Application Server (AS) is present as messages traveling between them are encrypted only but lack of a mechanism to calculate their integrity. Likewise, data integrity might be compromised as data encryption is performed in counter mode only and hence, a bit flipping attack over the ciphertext could be executed. Finally, some recommendations are listed by the researchers. First of all, to mitigate decrypt or replay attacks, it is important to validate that either AppNonce or DevNonce have been previously generated or to add counter instead of a random procedure; however, this last recommendation might allow an attacker to guess the next parameter to be used. Increasing the size of the fields that carry such information would help to avoid repetition. Second, to prevent DoS attacks it is recommended to associate a particular join-request with a join-accept message. Finally, confirming keys would allow to prevent a replay or decrypt attack anyhow, those session keys might be generated twice and hence such countermeasure would not be enough, so, it must combine with the previous mentioned recommendations. This research depicts vulnerabilities of LoRaWAN V1.0. Most of the analysis performed is based entirely over the specification but researchers have proved mathematically or practically

(through formulas) that most of the attacks are real and might be exploited by malicious users. Countermeasures proposed by the researchers are valid but might demand additional hardware resources over considering that end-node devices have a very limited computational capacity.

Key management and replay attacks are also identified as potential vulnerabilities in LoRaWAN and hence, a solution is proposed by You *et al.* (2018). The researchers aim to add additional security measures to the current steps of LoRaWAN 1.0 to increase its level of security by generating an authentication procedure between the end-node device and the Application Server (AS). The researchers propose the inclusion of a 3-step authentication confirmation between the end-node and the AS after the AppSKey has been generated. Also, there is a novel proposal for the DevNonce generation to obtain fresh join-request messages and prevent replay attacks. This approach claims to be secure as demonstrated by the researchers using ban logic and AVISPA tool. Also, it appears to be a low computational cost solution according to the tests performed. This solution has been implemented over a smart parking case study. Finally, although, the research described is based on Version 1.0, it could be applied to Version 1.1 as LoRaWAN still lacks of a proper end-to-end security that delivers privacy; however, the researchers state that performance testing should be performed to validate its feasibility. This research might be applied to the new version of LoRaWAN but it is important to consider that there are power and computing restrictions for its implementation.

A major concern for improving LoRaWAN security is battery consumption. For that reason, there are scientific works for increasing security in LoRaWAN that aim to reduce battery consumption (a major premise of IoT) as proposed by Tsai *et al.* (2018). The researchers consider this fact to optimize AES-128 and come up with a solution called Secure Low Power Communication (SeLPC) which is based on D-Box that are renewed after a certain period of time and adding it to the AES process to improve its performance without scarifying security. This approach is based on two major phases: key generation and data encryption process. The purpose of the first stage is to update the AppSKey and the S-Box of AES after a period of n days (which could be configured by the network administrator). To achieve such goal, enhanced version of DASS algorithm (used to handle S-Box) and D-Box generation are used. Finally, D-Box and AppSkey are updated every n days according to the definition adopted. Second, to perform data encryption researchers suggest that lieu to the fact that AppSKey and D-Box are updated frequently it will only be required to perform 5 rounds of AES-128 to encrypt the message to be sent. This approach is resistant to known-key attack as malicious user might have obtained a previous AppSKey but he still needs the D-Box and a newly updated AppSKey. Also, replay-attacks are not possible because the reply message is based on AppSKey and time parameter. Finally, although, an attacker could be able to sniff over the channel and obtain an older AppSKey he could not be able to decrypt the message as AppSKey is based on a time variable. This research focus on secure one key but as mentioned by the researchers it needs to be extended to secure NwkSKey and MIC-code generation. In terms of performance, researchers show that it might save around 26% of power consumption. Even though this approach is not specified for a particular version of LoRaWAN, it coud be applied over the current version.

J. Kim and J. Song discuss a novel approach to securely share cryptographic keys for protecting Device to Device (D2D) communication. Researchers mentioned that their research guarantees mutual authentication, integrity and confidentiality (Kim and Song, 2018). This research aims to support authentication between two devices interacting within a LoRaWAN system. The scheme proposed will generate two new messages (SecureD2DReq and SecureD2DAns) and will use NwkSKeys generated by the network server together with a device nonce to produce encryption keys and integrity keys. Although, this research does not directly address a vulnerability or a particular attack, it proposes a schema for increasing data rates. However, this approach needs to be tested over the new protocol specification.

To best of our knowledge the latest paper in regards of examining LoRaWAN 1.1 vulnerabilities is presented in (Eldefrawy *et al.*, 2019). The researchers use a tool called scyther which is a formal tool to verify the security of protocols (Anonymous, 2014). In this research, researchers prove in a formal way that there are issues in regards of key exchange in Version 1.0; however, according to the researchers, they have not found weaknesses in the current version of the LoRaWAN protocol. According to the findings, the OTAA procedure of Version 1.0 lacks of proper association between the end-device and the NS or AS. This is produced because join-request and join-accept are not properly acknowledged. On the other hand in terms of Version 1.1 researchers state that there might be security flaws in the AES algorithm using ECB for encrypting join-accept messages. Man-In-The-Middle-attack (MITM) are possible through the bit-flipping attack even in the new version of LoRaWAN as discussed by the researchers.

The problem is that messages are encrypted between the end-node and the servers but there is no mechanism to guarantee that messages sent between NS and AS are trustable in terms of integrity. According to the specification, NS and AS have to trust each other but there is no procedure described to achieve it. One of the most critical issues that has been denoted by the researchers is root key-preloading, it poses a threat as those keys could be extracted by a malicious user and hence, compromise the confidentiality of the information exchanged. Roaming capabilities of LoRaWAN may end up in MITM attacks as handover-roaming is present. Also, this feature might result in a fallback, since, handover-roaming is not present in the previous versions of LoRaWAN. Anyhow, the discussed vulnerabilities have not been tested over a real implementation to confirm if such weaknesses might represent a real risk to the protocol.

In spite of using a secure encryption algorithm like AES-128. LoRaWAN is susceptible to bit-flipping attacks. In this attack, a malicious user would be able to forge encrypted payloads to produce fake information. Anyhow, researchers by Lee *et al*. (2017) have proposed a shuffling method to prevent attackers exploiting such vulnerability. The procedure consists in two phases: shift phase where all the bytes perform a circular shift to the left and swap phase where the end-device swaps positions of the previously shifted bytes. Although, the approach seems to be secure it might generate some performance issues. Also, it is not clear what would happen with repeated messages and hence, they should have a different way of mixing bytes every time. Besides, an integrity check must be in place to prevent data corruption.

RESULTS AND DISCUSSION

For this research we have considered 45 sources of information which are distributed as shown in Fig. 7. The results obtained showed that mostly papers are from conference proceedings (42% approx.) and journals (29% approx.). This shows that research community is dedicating to evaluate the vulnerabilities around LoRaWAN protocol. On the other hand, only 4% of the reviewed information belongs to reports from the industry in regards of the research topic.

According to our findings, the highest concentration of papers is present between 2017 and 2018. A tendency could be observed in regards of interest of vulnerabilities in LoRaWAN as shown in Fig. 8. Although, the numbers of papers have been reduced from 2017-2018, it might not mean that the protocol is not of interest, unlike it could

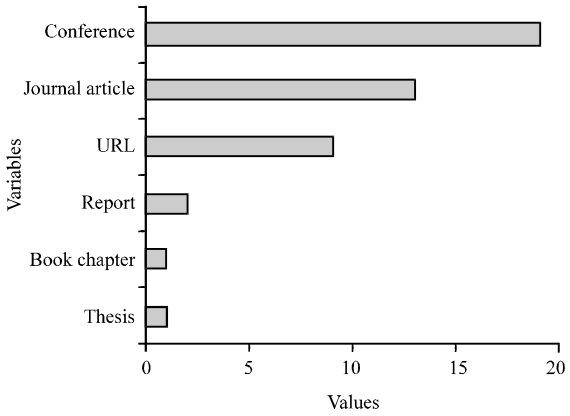

Fig. 7: Publication types (Information source)

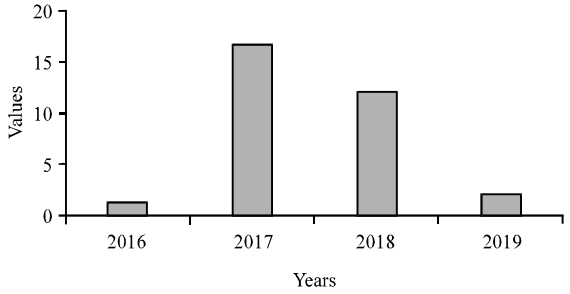

Fig. 8: Publications distribution per year

obey to the fact that a new version is in place and has barely more than 1 year and a half. In fact, LoRaWAN was updated in October 2017 to a new specification 1.1 and apparently most vulnerabilities from previous Version 1.0.2 has been addressed (Donmez and Nigussie, 2018). However, it is not wise to ensure that it is "vulnerability-free" protocol as technology is constantly evolving and new attacking techniques are developed every day.

To the best of our knowledge, there are no public exploits listed within hacker's community conferences (DEFCON (INC., n.d.) and Black Hat (UBM., 2018) or confirmed vulnerabilities in regards of LoRaWAN as reviewed in CVE (MC., 2018). Our search threw one entry related to reversing LoRa PHY with the aim of a tool called gr-lora which is an open source tool used to accelerate IoT development and security research (Knight and Seeber, 2016).

LoRaWAN new specification seems to have considered important aspects to provide better security; however, there are still things to enforce and improve such as demanding secure channels as a non-negotiable requirement. Likewise, physical access to devices is still an open issue that might compromise keys and therefore,

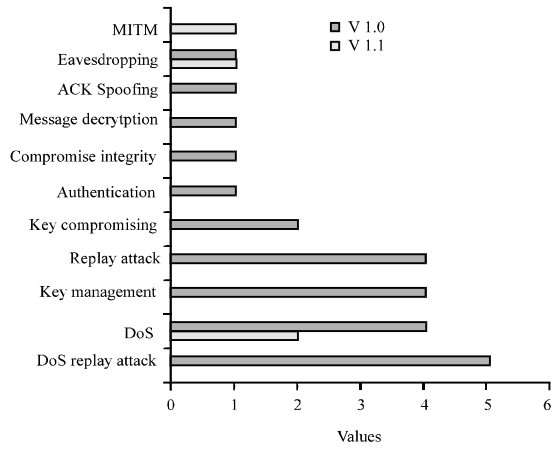

Fig. 9: LoRaWAN vulnerabilities by protocol version

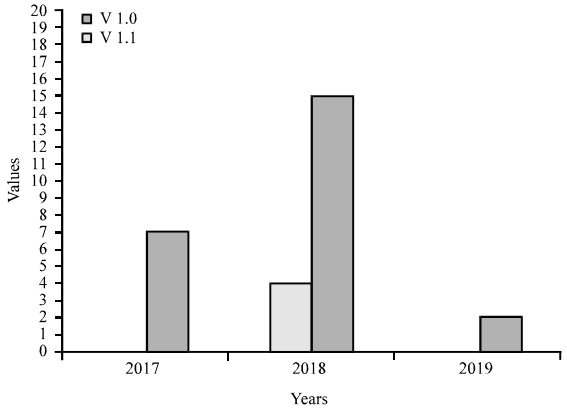

Fig. 10: LoRaWAN vulnerabilities grouped by year

information, although, the applications of LoRaWAN are sensor oriented in a near future there might devices capable of receive information and then new threats might appear.

Although, some analysis performed over the security of the protocol are still made only by assuming scenarios and reviewing the specification, there is a formal scenario (Eldefrawy *et al*., 2019) that proves its security with the aim of a tool. Anyhow, the findings identified by the researchers should be tested over the infrastructure to validate vulnerability exploitability.

From the review performed it could be said that LoRaWAN is mostly affected by replay attacks (according to the researchers they might end into a denial of service attack leaving nodes uncommunicated), key management issues in both specifications and denial of service attacks either through jamming or by ignoring nodes/servers lieu to improper join request-accept confirmation as compiled through the research performed and briefly summarized by Chatzigiannakis *et al*. (2018), Hague (2016), Krejci *et al*. (2017) and deeply discussed in (Van Es, 2018). Figure 9 shows a summary of the attacks identified by the research community in both LoRaWAN versions. Some of the attacks listed are related between each other. For instance, if an attacker is able to obtain root keys (AppKey and NwkKey) he/she might be able to decrypt messages. Also, even if there AES-128 encryption in place a malicious user might perform a bit-flipping attack to compromise information integrity. Besides, in spite of such cryptographic level it is still possible to perform MITM attacks or channel eavesdropping.

Although, authentication has not been widely discussed over the works review it represents a potential issue, since, the specification does not specify how to recognize or validate an end-node authenticity. Researchers by Olsson and Finnsson (2017) briefly states that an attacker might inject packets to the system taking advantage of such weakness.

According to the results of our research, scientific community is working on finding vulnerabilities and securing this protocol. Moreover, the new specification of LoRaWAN as described in the previous study has vulnerabilities which have not been exploited yet. There are still vulnerabilities from the previous specification which have been exploited and due to the backward compatibility, they might affect the new version. Anyhow, this is not the last and official list, new threats might appear in the future as the technology becomes more popular. After the performed review, it could be said that LoRaWAN 1.1 is more secure than the previous version, the following (Fig. 10) help us to sustain such affirmation. Although, Version 1.0 is about 4 years old and considering that Version 1.1 is recently new, scientific community is still reviewing the state of security of such version. Furthermore, as soon as the new version was launched, some weaknesses were found.

An important concern that has caught our attention from the research performed is that the protocol does not address the fact of having rogue gateways within a LoRaWAN infrastructure to collect data from end-node devices or even worse, turning them into zombies or malware carriers for attacking IP networks. Considering this scenario, all messages sent from end-node devices are properly encrypted with AES-128 to provide a certain level of confidentiality; however, this mechanism can be misused as malicious packets might be sent to compromise other points of network. In fact, all packets would be treated as trusted and be passed to the next node. With the aforementioned scenario, it would be required to have a device like an Intrusion Detection System (IDS) that could decrypt, inspect, discard and

forward such messages. However, to achieve such goal would demand that such device might contain some essential keys and network session keys like AppKey, NwkKey, AppSkey, NwkSkey among others. In this scenario, the problem that appears is that this single point will know all the keys for package inspection but this represents a new threat because if it is compromised, all the keys contained will therefore be compromised as well. Hence, a proper enrollment process for end-node devices has to be in place, this task should be executed by the gateway which is in charge of attaching every end-node to the IP network. It is important to remark that gateways only scan the spectrum in search of LoRa packets from end-node devices and then forward them to a network service.

In regards of creating awareness of security issues in LoRaWAN, there is a work published that aims to teach users the potential threats of such protocol by using a virtual reality scenario where users can interact and understand how different keys are generated as well as the procedures involved. Researchers have addressed OTAA and ABP procedures with all elements involved to make it easy comprehend the weaknesses and state of security of LoRaWAN before implementing it without prior knowledge (Liagkou *et al*., 2019). Although, this research does not address or discuss a particular vulnerability, on the contrary it presents a learning and awareness-raising scenario for the end user. Likewise, researches like (Oniga *et al*., 2017b) try to offer a set of recommendations or best practices that could be adopted when implementing a LoRaWAN network. Those recommendations are based on identified vulnerabilities as well as considerations for the IP network.

From our perspective, to increase the security of the protocol, it is mandatory to create/reinforce policies and standards to support the design and construction processes of end-node devices and gateways. LoRa Alliance is a good initiative that requires a solid participation of the research community as well as the industry. Recently, LoRa-Alliance have released some recommendations for Data Block Transport Specification, Firmware Update Over-the-Air, Layer Clock Synchronization Specification and Remote Multicast Setup Specification (LA., 2017; Raza *et al*., 2017; LA., 2019a, b) to address important features that have not been discussed over the whole specification.

CONCLUSION

After reviewing several papers on vulnerabilities, security issues and countermeasures on LoRaWAN, we can conclude that the last version of the protocol has addressed several issues (common threats for IoT environments) that have been identified in the previous version of the protocol, however, there are some vulnerabilities that have been recently identified through protocol analysis and simulations. The remaining vulnerabilities have not been practically exploited yet but they still represent an important threat to the LoRaWAN environment.

The most remarkable improvement in the security of LoRaWAN is the introduction of the new key called NwkKey proposed by Kim and Song (2017b). This new key opened the opportunity to generate additional keys and servers. Indeed, more types of servers appeared leading to a clear separation of duties.

All in all, LoRaWAN appears to be a secure protocol that has strong security features for protecting information. However, there is still work to do in regards of building a proper key distribution schema as storing keys from factory is still an open issue, if the device is physically compromised. Likewise, there is still work to do in regards of designing a proper trust schema between several servers of the environment to prevent attacks against integrity and confidentiality of the information. In addition, network security mechanisms such as VPN, firewall or IPS must be in place to prevent attacks containing malicious payloads sent from the LoRa network could compromise the whole infrastructure (Oniga *et al*., 2017a). Finally, there will always be a lot to do when enhancing the level of security of any protocol even, if there are already secure mechanisms in place.

ACKNOWLEDGEMENT

The researchers gratefully acknowledge the financial support provided by the Escuela Politecnica Nacional, for the development of the project PIJ-17-08-"Diseno e implementacion de un sistema de parqueadero inteligente".

REFERENCES

Anonymous, 2014. The Scyther tool. Helmholtz Center for Information Security (CISPA), Saarbrucken, Germany. https://people.cispa.io/cas.cremers/scyther/

Anonymous, 2018a. What is LoRa?. Semtech Corporation, Camarillo, California, USA. https://www.semtech.com/lora/what-is-lora

Anonymous, 2018b. Zotero 5.0 for windows. Zotero, Vienna, Virginia. https://www.zotero.org/download/

Aras, E., G.S. Ramachandran, P. Lawrence and D. Hughes, 2017a. Exploring the security vulnerabilities of LoRa. Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), June 21-23, 2017, IEEE, Exeter, UK., ISBN:978-1-5386-2202-5, pp: 1-6.

Aras, E., N. Small, G.S. Ramachandran, S. Delbruel and W. Joosen *et al*., 2017b. Selective jamming of LoRaWAN using commodity hardware. Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, November 7-10, 2017, ACM, Melbourne, Victoria, Australia, ISBN:978-1-4503-5368-7, pp: 363-372.

Avoine, G. and L. Ferreira, 2018. Rescuing LoRaWAN 1.0. Financial Cryptography Data Secur., 3: 779-787.

Butun, I., N. Pereira and M. Gidlund, 2018. Analysis of LoRaWAN v1. 1 security. Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, June 25, 2018, ACM, Los Angeles, California, ISBN:978-1-4503-5857-6, pp: 1-6.

Chatzigiannakis, I., V. Liagkou and P.G. Spirakis, 2018. Brief Announcement: Providing End-to-End Secure Communication in Low-Power Wide Area Networks. In: Cyber Security Cryptography and Machine Learning, Dinur, I., S. Dolev and S. Lodha (Eds.)., Springer, Cham, Switzerland, ISBN:978-3-319-94146-2, pp: 101-104.

Danish, S.M., A. Nasir, H.K. Qureshi, A.B. Ashfaq and S. Mumtaz *et al*., 2018. Network intrusion detection system for jamming attack in lorawan join procedure. Proceedings of the 2018 IEEE International Conference on Communications (ICC), May 20-24, 2018, IEEE, Kansas City, Missouri, USA., ISBN:978-1-5386-3181-2, pp: 1-6.

Donmez, T.C.M. and E. Nigussie, 2018. Security of LoRaWAN v1. 1 in backward compatibility scenarios. Procedia Comput. Sci., 134: 51-58.

Eldefrawy, M., I. Butun, N. Pereira and M. Gidlund, 2019. Formal security analysis of LoRaWAN. Comput. Networks, 148: 328-339.

GI., 2015. Gartner says 6.4 billion connected things will be in use in 2016, up 30 percent from 2015. Gartner, Inc., Stamford, Connecticut, USA. https://www.gartner.com/en/newsroom/press-releases/2014-11-11-gartner-says-nearly-5-billion-connected-things-will-be-in-use-in-2015

Hague, T., 2016. Security review of LoRaWAN networks. DCC, Inc., Avon, Indiana.

Iskhakov, S., R. Meshcheryakov, A. Iskhakova and S. Bondarchuk, 2017. Analysis of vulnerabilities in low-power wide-area networks by example of the LoRaWAN. Proceedings of the 4th International Research Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2017), December 5-8, 2017, Atlantis Press, Paris, France, ISBN:978-94-6252-432-3, pp: 334-338.

Kim, J. and J. Song, 2017a. A dual key-based activation scheme for secure LoRaWAN. Wireless Commun. Mob. Comput., 2017: 1-12.

Kim, J. and J. Song, 2017b. A simple and efficient replay attack prevention scheme for LoRaWAN. Proceedings of the 2017 the 7th International Conference on Communication and Network Security, November 24-26, 2017, ACM, Tokyo, Japan, ISBN:978-1-4503-5349-6, pp: 32-36.

Kim, J. and J. Song, 2018. A secure device-to-device link establishment scheme for LoRaWAN. IEEE. Sens. J., 18: 2153-2160.

Knight, M. and B. Seeber, 2016. Decoding LoRa: Realizing a modern LPWAN with SDR. Proceedings of the 6th GNU Radio Conference Vol. 1, September 6, 2016, Boulder, Colorado, pp: 1-5.

Krejci, R., O. Hujnak and M. Svepes, 2017. Security survey of the IoT wireless protocols. Proceedings of the 2017 25th International Conference on Telecommunication Forum (TELFOR), November 21-22, 2017, IEEE, Belgrade, Serbia, ISBN:978-1-5386-3074-7, pp: 1-4.

Kuo, C.T., V. Chang and C.L. Lei, 2017. A feasibility analysis for edge computing fusion in LPWA IoT environment with SDN structure. Proceedings of the 2017 International Conference on Engineering and Technology (ICET), August 21-23, 2017, IEEE, Antalya, Turkey, ISBN:978-1-5386-1950-6, pp: 1-6.

Kusen, E. and M. Strembeck, 2017. Security-related research in ubiquitous computing-results of a systematic literature review. Cryptography Secur., 1: 1-12.

LA., 2017. LoRaWAN® Specification v1.1. LoRa Alliance, Berlin, Germany. https://lora-alliance.org/resource-hub/lorawanr-specification-v11

LA., 2019a. LoRaWAN application layer clock synchronization specification v1.0.0. LoRa Alliance, Berlin, Germany. https://lora-alliance.org/sites/default/files/2018-09/application_layer_clock_synchronization_v1.0.0.pdf

LA., 2019b. LoRaWAN remote multicast setup specification v1.0.0. LoRa Alliance, Berlin, Germany. https://lora-alliance.org/resource-hub/lorawanr-remote-multicast-setup-specification-v100

Lee, J., D. Hwang, J. Park and K.H. Kim, 2017. Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. Proceedings of the 2017 International Conference on Information Networking (ICOIN), January 11-13, 2017, IEEE, Da Nang, Vietnam, ISBN:978-1-5090-5125-0, pp: 549-551.

Liagkou, V., C. Stylios and D. Salmas, 2019. VR training model for exploiting security in LPWAN. Procedia CIRP., 79: 724-729.

MC., 2018. CVE-search results. MITRE Corporation, McLean, Virginia, USA. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=lorawan

Mekki, K., E. Bajic, F. Chaxel and F. Meyer, 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT. Express, 5: 1-7.

Miller, R., 2016. Lora security: Building a secure Lora solution. MWR InfoSecurity Limited, Basingstoke, USA. https://labs.mwrinfosecurity.com/publications/lo/

Na, S., D. Hwang, W. Shin and K.H. Kim, 2017. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. Proceedings of the 2017 International Conference on Information Networking (ICOIN), January 11-13, 2017, IEEE, Da Nang, Vietnam, ISBN: 978-1-5090-5125-0, pp: 718-720.

Naoui, S., M.E. Elhdhili and L.A. Saidane, 2016. Enhancing the security of the IoT LoraWAN architecture. Proceedings of the 2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), November 22-25, 2016, IEEE, Paris, France, ISBN:978-1-5090-2671-5, pp: 1-7.

Olsson, K. and S. Finnsson, 2017. Exploring LoRa and LoRaWAN: A suitable protocol for IoT weather stations?. Master Thesis, Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden.

Oniga, B., V. Dadarlat, E. De Poorter and A. Munteanu, 2017a. A secure LoRaWAN sensor network architecture. Proceedings of the 2017 IEEE International Conference on SENSORS, October 29-November 1, 2017, IEEE, Glasgow, UK., ISBN: 978-1-5090-1013-4, pp: 1-3.

Oniga, B., V. Dadarlat, E. De Poorter and A. Munteanu, 2017b. Analysis, design and implementation of secure LoRaWAN sensor networks. Proceedings of the 2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), September 7-9, 2017, IEEE, Cluj-Napoca, Romania, ISBN:978-1-5386-3369-4, pp: 421-428.

Raza, U., P. Kulkarni and M. Sooriyabandara, 2017. Low power wide area networks: An overview. IEEE. Commun. Surv. Tutorials, 19: 855-873.

Sanchez-Iborra, R., J. Sanchez-Gomez, S. Perez, P. Fernandez and J. Santa *et al*., 2018. Enhancing lorawan security through a lightweight and authenticated key management approach. Sens., 18: 1-18.

Sung, W.J., H.G. Ahn, J.B. Kim and S.G. Choi, 2018. Protecting end-device from replay attack on LoRaWAN. Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), February 11-14, 2018, IEEE, Chuncheon-si, South Korea, ISBN:978-1-5386-4688-5, pp: 167-171.

Tomasin, S., S. Zulian and L. Vangelista, 2017. Security analysis of LoRaWAN join procedure for Internet of Things networks. Proceedings of the 2017 IEEE International Workshops on Wireless Communications and Networking (WCNCW), March 19-22, 2017, IEEE, San Francisco, California, USA., ISBN:978-1-5090-5909-6, pp: 1-6.

Tsai, K.L., Y.L. Huang, F.Y. Leu, I. You and Y.L. Huang *et al*., 2018. AES-128 based secure low power communication for LoRaWAN IoT environments. IEEE. Access, 6: 45325-45334.

UBM., 2018. Black hat archives. UBM Plc, London, UK. https://www.blackhat.com/html/archives.html

Van Es, E., 2018. LoRaWAN vulnerability analysis. MCS Thesis, Open University of the Netherlands, Heerlen, Netherlands.

Van Es, E., H. Vranken and A. Hommersom, 2018. Denial-of-service attacks on LoRaWAN. Proceedings of the 13th International Conference on Availability, Reliability and Security, August 27-30, 2018, ACM, Hamburg, Germany, ISBN:978-1-4503-6448-5, pp: 1-17.

Yang, X., E. Karampatzakis, C. Doerr and F. Kuipers, 2018. Security Vulnerabilities in LoRaWAN. Proceedings of the 2018 IEEE/ACM 3rd International Conference on Internet-of-Things Design and Implementation (IoTDI), April 17-20, 2018, IEEE, Orlando, Florida, USA., ISBN:978-1-5386-6313-4, pp: 129-140.

You, I., S. Kwon, G. Choudhary, V. Sharma and J.T. Seo, 2018. An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system. Sens., 18: 2-32.