Towards Securing LoRaWAN ABP Communication System

Hassan N. Noura[1,2], Ola Salman[1], Tarif Hatoum[2], Mohammad Malli[2] and Ali Chehab[1]
[1]*American University of Beirut, Department of Electrical and Computer Engineering, Lebanon*
[2]*Arab Open University, Department of Computer Sciences, Beirut, Lebanon*

Keywords: IoT, LoRaWAN, ABP, OTAA, Security Attack, Lightweight Security Solution.

Abstract: A large number of power-constrained devices will be connected to the Internet of Things (IoT). Deployed in large areas, the battery-powered IoT devices call for power efficient and long range communication technologies. Consequently, the Low Power Wide Area Networks(LPWAN) were devoted to being the key IoT enablers. In this context, LoRaWAN, an LPWAN technology, is one of the main IoT communication protocols candidates. However, LoRaWAN suffers from different security and privacy threats. These threats lead to several availability, authentication, and privacy attacks. In this paper, we present efficient countermeasures against two well-known ABP attacks (eavesdropping and replay). The proposed solution aims at making LoRa ABP end-devices safer, more secure and more reliable. In fact, the proposed solution is based on the dynamic key derivation scheme. We presented two variants of dynamic key derivation: counter-based and channel information-based. A set of security and performance tests shows that the proposed countermeasures present low overhead in terms of computation and communication resources with a high level of security.

1 GENERAL DESCRIPTION

Recently, the LoRaWAN technology is presented as key enabler for the IoT applications that require the transmission and reception of a a small amount of data at a low date rate within a range of few Kilometers. LoRaWAN data rate varies between 0.3 to 50 kbps, depending on both range and interference. LoRaWAN uses a wide bandwidth which helps in resisting against interference and noise, and achieving high power efficiency. Besides, it uses specific frequencies which are 868MHZ and 900MHZ, with the transmission range being dependent on the environment.

The LoRaWAN architecture is based on the star topology as shown in Figure 1. The IoT devices are connected to the LoRaWAN end-devices (EDs), which are directly connected to one (or more) gateway(s). Each gateway (GW) is connected to the network server(NS), which can be connected to one or more application servers(AS). In fact, the connection between LoRaWAN EDs and GWs is a LoRaWAN communication, whilst the connection between the GW and the AS is a traditional IP connection.

Mainly, an ED can be connected to LoRaWAN by using one of two activation modes, that can be Over-The-Air-Activation (OTAA) or Activation by Personalization (ABP). After activation, the EDs communicate the messages, that are authenticated and encrypted, by using a network key *NwSKey* and application key *AppSKey*, respectively with the NS. The NS knows the *NwSKey* of all EDs, while the AS knows the *AppSKey* of all EDs. However, the difference between the ABP and the OTAA is that in ABP, all the secret keys and identifiers are static, and they are all allocated at the ED. In addition, with ABP, the EDs are connected to the NS directly without any request. However, in OTAA, a join procedure is mandatory for the ED to connect to the network. In addition, in OTAA, the session keys are updated for each new session.

1.1 Problem Formulation

In LoRaWAN v1.1, new security enhancements are introduced. However, given that the root keys are static and the identifiers (e.g. JoinUI, DevNonce, etc.) used to generate the session keys are transmitted in plaintext, side channel and node capture attacks are still possible. Thus, both LoRaWAN v1.0 and v1.1 suffer from availability, integrity and confidentiality attacks in both ABP and OTAA activation modes (Eldefrawy et al., 2019). In this paper, we will focus on the ABP eavesdropping and replay attacks.

1.2 Motivation

LoRaWAN is a wireless technology that permits the connection of constrained IoT devices. These IoT de-

Noura, H., Salman, O., Hatoum, T., Malli, M. and Chehab, A.
Towards Securing LoRaWAN ABP Communication System.
DOI: 10.5220/0009561104400447
In *Proceedings of the 10th International Conference on Cloud Computing and Services Science (CLOSER 2020)*, pages 440-447
ISBN: 978-989-758-424-4

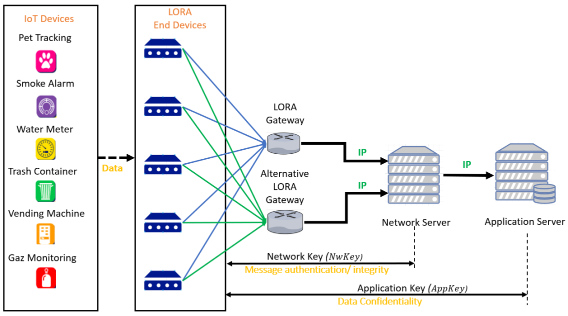


Figure 1: LoRaWAN Topology.

vices include sensors and embedded devices in automobiles, homes, roads and bridges, appliances and farms equipment. These devices generate different types of data, changing the way the data is produced and experienced. IoT obviously represents a great opportunity for advances in data analysis (Verma et al., 2017). The collection and processing of data from IoT devices by the application servers is gaining attention, except from a security perspective.

The security mechanism designed to protect communications must provide appropriate assurances in terms of confidentiality, integrity, authentication, and non-repudiation of information flow. In fact, the IoT security is very critical in terms of protection of data transfer between the end-devices and the servers via the transparent gateways. Such security problems are related to different types of attacks which may jeopardize the data transmission process between the IoT devices and the network (Salman et al., 2018; Salman et al., 2015; Salman et al., 2017).

1.3 Contributions

This paper focuses on the design of efficient countermeasures against eavesdropping and replay attacks for LoRaWAN in the ABP activation mode. The main goal of this work is to reach high level of security with the minimum possible resources and latency requirements.

A new efficient, flexible, lightweight and secure dynamic key derivation algorithm is proposed for LoRaWAN EDs. The strength of the proposed cipher scheme is that it employs the dynamic key approach and an update function that are iterated only when the session counter reaches the maximum value. These operations are designed to require minimum number of operations and to preserve the desirable cryptographic performance. To accomplish this objective, the dynamic key approach is employed, and dynamic network and application keys are produced for each reset operation. The network and application dynamic keys depend on the static network key along with the application secret key, in addition to a reset counter which is incremented by one for each reset. The dynamic key approach makes the collected traffic non-useful in the next reset session, which consequently prevents the replay or eavesdropping attacks. In addition, the proposed solution ensures a good cryptographic performance while requiring a low computational complexity.

1.4 Organization

The rest of this paper is organized as follows. In Section 2, we review the previous work proposing cryptographic solutions to enhance the LoRaWAN security. The different classes of LoRaWAN EDs in addition to the ABP activation mode are described in Section 3. In Section 4, LoRaWAN security attacks are explained and illustrated. Then, in Section 5, the two variants of the proposed countermeasure, which is based on a dynamic key derivation algorithm, are described. Then, a security analysis is included in Section 6 to show the robustness of the proposed countermeasure, which makes the LoRaWAN security attacks inapplicable. Moreover, the performance of the proposed countermeasure is analysed in Section 7. Finally, the conclusions along with the directions for future work are presented in Section 8.

2 RELATED WORK

In this section, we review the cryptographic based solutions for the LoRaWAN security threats. The bit flipping attack consists of changing one bit in the ciphertext without decrypting it. This attack is possible due to the use of AES in the counter mode. A solution to shuffle the ciphertext is proposed in (Lee et al., 2017). A dual activation solution is proposed (Kim and Song, 2017a). This solution consists of generating new keys $Nwk_{S}Key$ and $App_{S}Key$ to thwart the node capture and side channel attacks. A replay attack prevention is proposed by modifying the reset condition in (Kim and Song, 2017b). In this case, the join procedure is performed only when the *NwkSKey* is lost at the ED . Another work considering the protection of EDs from the replay attack is done in (Sung et al., 2018). Measuring the Received Signal Strength Indicator (RSSI) of the received join request signal, the NS can differentiate between the user and the attacker. However, this method is not reliable when the attacker and the user are at the same distance. In addition, the LoRaWAN ED might not be at fixed position. An AES scheme for *AppSKey* and D-Box update each k days is proposed in (Tsai et al., 2018).

The proposed solution is based on a lightweight and efficient AES version. Another work that considers the management of *NwkSKey* and *AppSKey* by introducing an adaptation security layer protocol based on Ephemeral Diffie–Hellman Over COSE (EDHOC) is proposed in (Sanchez-Iborra et al., 2018). However, the considered device for performance testing does not conform with many of the IoT constrained devices capabilities. In (Xia et al., 2018), a key management framework based on a trusted Key Distribution Server (KDS) based scheme is proposed. Introduced in (Ruotsalainen and Grebeniuk, 2018; Zhang et al., 2018), the feasibility of secure key generation based on the wireless channel measurements (i.e. Received Signal Strength Information (RSSI)) is conducted in (Xu et al., 2019; Xu et al., 2018). Even though LoRaWAN v1.1 presents new security measures that aim at enhancing the LoRaWAN security, however the confidentiality attacks are still possible. Thus, the update of the root keys used for deriving the session keys is necessary to avoid the session keys disclosure. For this aim, a Rabbit cipher-stream based key derivation function is proposed in (Han and Wang, 2018) to update the root keys at the ED. In this paper, a dynamic key derivation scheme is proposed to prevent ABP replay and confidentiality attacks. Two variants of this scheme are presented: a counter-based and a piece of channel information-based. By using the proposed dynamic key approach, different dynamic network and application keys are used for each reset time. Therefore, different keystream will be produced, since the application key is changed and consequently different ciphertext will be produced. This makes the confidentiality attacks unfeasible. In parallel, by using a different network key, previously received messages will not be validated, which consequently prevents replay attack. The choice of the convenient scheme (counter-based or channel information-based) is based on the ED capabilities.

3 LoRaWAN BACKGROUND

In this section, the different classes of LoRaWAN EDs are first presented, then we explain the ABP activation mode. Note that Table 1 represents the notations used in this paper.

3.1 LoRaWAN End-Devices

The LoRaWAN EDs are the IoT devices connected to the LoRa network. These devices are connected to the LoraWAN GW and send data to the LoRa network. Being sensors that measure pressure, velocity, humidity, temperature, vibration, etc., the LoRaWAN EDs are divided into three classes: A, B, and C, based on the *MAC* layer operation (Aras et al., 2017; Augustin et al., 2016; Vangelista et al., 2015).

Table 1: Table of Notations.

Symbol	**Definition**
CR	Coding Rate
RC	Reset Counter
NwkSKey	Network Secret Key
AppSKey	Application Secret Key
FNwkSIntKey	MAC layer network integrity key
SNwkSIntKey	Network session encryption key
NwkSEncKey	Forwarding network session integrity key
SSK	Static secret key

3.2 Activation By Personalization (ABP)

Unlike OTAA, the ABP activation mode does not include a join procedure. In this case, the ED can send and receive messages without the need to be authenticated first by the network. However, for confidentiality, the messages are encrypted and authenticated using session keys preloaded inside each ED. In fact, each ED has its unique session keys *NwkSKey*, and *AppSKeyy*. Moreover, in LoaRaWAN v1.1, three keys are introduced which are: *FNwkSIntKey*, *SNwkSIntKey*, and *NwkSEncKey*. This way, if any ED is compromised, the security of the other EDs communications will not be compromised. In case of ED reset, the ED sends the *ResetIndMAC* command in *FOpt* for all the uplink messages, and waits for the *Resetconfcommand*. Otherwise, the ED sends and receives the messages.

4 LoRaWAN ATTACKS

In this section, we describe the main LoRaWAN security attacks considered in the literature. Mainly, we have two types of attacks that we aim at defending by our proposed solution, namely the replay and eavesdropping attacks. Note that these attacks are still valid for LoRaWAN v1.1. In addition, given that LoRaWAN v1.0 is still in use, it is important to consider both LoRaWAN v1.0 and v1.1 vulnerabilities when proposing a new security solution.

4.1 Eavesdropping Attack

To ensure the message confidentiality, LoRaWAN employs AES-128 in a counter mode. Thus, if two ciphertexts are being encrypted by the same key-stream

cipher ($C1 = P1 \oplus K$ and $C2 = P2 \oplus K$), the attacker is able to know the exclusive or (XOR) of the plaintext messages by XORing the collected ciphertexts ($C1 \oplus C2 = P1 \oplus P2$). Thus, in the ABP mode, where the session keys are static, when the counter is reset, the same key-stream cipher is obtained (Tsai et al., 2018; Salinesi et al., 2011; Kuipers,).
Note that this attack is only possible in ABP mode, given that in OTAA mode, the session keys are updated after a counter reset. In fact, to have a full knowledge of the communicated messages, the attacker needs to know or choose one of the plaintexts $P1$ or $P2$ (Yang et al., 2018; Mundt et al., 2018). Therefore, the confidentiality of next communication messages is broken.

4.2 Replay Attack

The ABP replay attack consists of replaying old packets by the attacker. As the used session keys are static, the attacker can replay the packets when the counter is reset to 0 (Sung et al., 2018). In this case, the attacker stores the uplink messages and replay them when the counter is reset (Tomasin et al., 2017; Salinesi et al., 2011; Na et al., 2017; Kim and Song, 2017b).

5 PROPOSED DYNAMIC KEY BASED SOLUTION

In order to defend against replay attacks, some simple countermeasures exist such as the use of timestamps, onetime passwords, and challenge-response cryptography. Nevertheless, these schemes are inconvenient, considering the vulnerabilities to which challenge-response protocols are susceptible to. In addition, to defend the key related attacks, key dynamicity is essential to limit the attack influence and the attacker capabilities.

The LoRaWAN specification explicitly warns developers about generating secure network and application keys: **Each device should have a unique set of ”NwkSKey” and ”AppSKey”. Compromising the keys of one ED should not compromise the security of the communications of other devices (Sisinni et al., 2018)**. The process to build those keys cannot be derived in any way from any publicly available information such as the Node address.

The characteristics of the proposed countermeasure are listed in the following:

- **Lightweight Countermeasure Scheme:** The proposed scheme uses a minimum number of iterations (operations), and it is only applied during the reset operation. Our aim is to make the solution lightweight towards reducing the required memory and power consumption.
- **Flexibility:** The proposed countermeasure is flexible, in which we have two simple countermeasure variants(depends on LoRaWAN ED class). The computational complexity of the first variant is low compared to the second one, while the security level of the second one is higher compared to the first one
- **Simple Hardware and Software Implementations:** The proposed key derivation function uses logical exclusive OR and can also use any secure hash function (second variant), which renders the corresponding hardware and software implementations of the proposed key derivation scheme to be simple and efficient.
- **Dynamic Key Approach:** In contrast to the existing cipher solutions, the proposed approach is based on dynamic keys, which is variable and changes in a pseudo-random manner after each new reset operation. In addition, changing the dynamic key produces different ciphertext and MIC(s). The dynamic nature of the proposed cipher provides high robustness against any kind of attacks (Naoui et al., 2016).
- **High Level of Security.**

5.1 Counter-based Countermeasure

The produced dynamic key depends on the static secret keys that are embedded in the ED, in addition to employing a reset counter number CR. The dynamic network and application secret keys for EDs of class A and B is presented in the following:

$$DSK = SSK \oplus CR \tag{1}$$

In fact, the proposed technique mixes (exclusive or) the static secret key (SSK) with the number of sessions CR towards producing the dynamic secret keys (DSK). The update of the dynamic secret keys for class C EDs is presented in the following:

$$DSK = h(SSK \oplus CR) \tag{2}$$

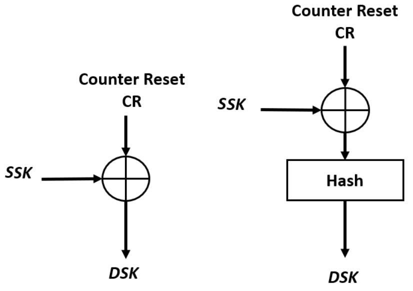
where h represents any secure cryptographic hash function, such as SHA-512.

Each corresponding output (mixing between static key and counter reset) is hashed to produce a dynamic session key (DSK) for each new reset session as described in the previous equation.

Note that the SSK and the corresponding DSK, as shown in Figure 2, represent the static session keys and their corresponding dynamic keys, respectively.

These session keys include: $NwkSKey$, $AppSKey$, $FNwkSIntKey$, $SNwkSIntKey$, and $NwkSEncKey$.

However, the difference between the previous dynamic key derivation functions and our proposed solution is that we use a secure cryptographic hash function for EDs of class C, which have better characteristics in terms of resources and computation compared to EDs of class A and B.



(a) (b)

Figure 2: The proposed Counter-based dynamic key derivation scheme for LoRaWAN EDs: (a) for class A and B, and (b) for Class C, respectively.SSK represents the static network or application key, while DSK represents the dynamic network or application keys.

5.2 Physical Channel based Countermeasure

The main motivation behind this variant is to avoid the limitations of key-less/static key techniques and benefit from the dynamic and random nature of the physical channel. This solution ensures the desired dynamic key approach by using channel parameters, which can lead to enhance the security level.

Figure 3 illustrates the proposed key derivation function that takes as inputs a network or application secret key SSK and a nonce N_o, which is updated from the physical channel parameters for every new session. In fact, the **Nonce** N_o can be obtained by combining several channel parameters (Noura et al., 2018) (such as Channel State Information (CSI) and Received Signal Strength (RSS)). These parameters change in a dynamic manner, and we assume that a good synchronization is realized between emitter and transmitter, which allows each entity to derive the same nonce separately (Noura et al., 2019b; Noura et al., 2019c; Noura et al., 2019a). Moreover, in order to generate the nonce, channel parameters (real numbers), such as the CSI and RSS, are first converted to a sequence of bytes, then hashed to obtain the required nonce. The hash function is introduced here towards reaching a high nonce sensitivity against any slight change in channel parameters. The secure hash function ($SHA-512$) is selected for this step, since it possesses the best and most desirable cryptographic hash properties (strong collision).

Then, the nonce is XORed with the static network and application secret keys to derive the dynamic network and application keys. It is important to generate a new nonce for each new session.

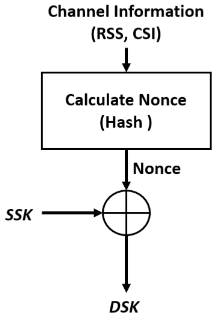


Figure 3: Proposed dynamic key generation steps.

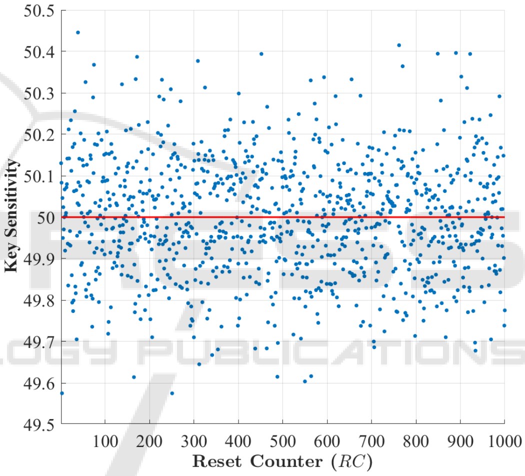


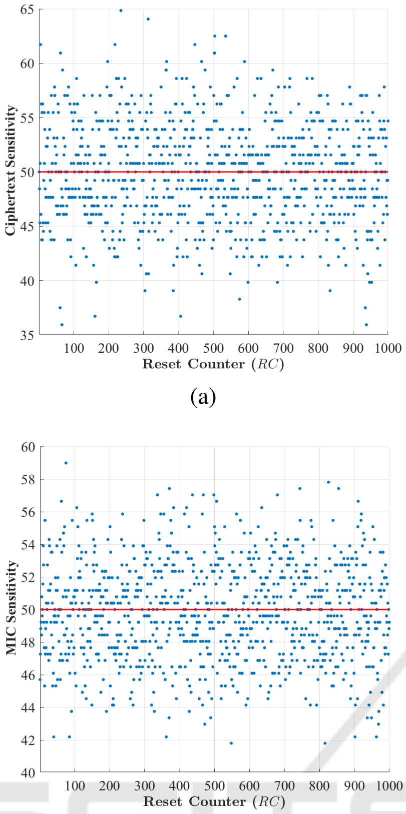
Figure 4: Variation of the dynamic key sensitivity in function of reset counter (RC) by using the proposed countermeasure for LoRaWAN end-devices classes C (uses SHA-256).

6 SECURITY ANALYSIS

In this section, the security level of the proposed key derivation scheme is analyzed and assessed. More specifically, the produced update network and applications keys should reach a high level of randomness, uniformity, and sensitivity. Randomness and uniformity tests in addition to sensitivity tests are applied to evaluate the security level of the proposed solution.

6.1 Dynamic Key Sensitivity

In this test, the sensitivity of the secret key is analysed, in order to assess the proposed scheme's robust-



(a)

(b)

Figure 5: Variation of the ciphertext and MIC sensitivity in function of reset counter (RC) by using the proposed countermeasure for LoRaWAN end-devices classes A and B.

ness against weak keys and related key attacks. More specifically, a one bit change in the network or application secret key should result in a 50% different set of ciphertext or MIC, respectively. Consequently, two (network or application) secret keys, DSK_1 and DSK_2 which differ by only one bit, are used to encrypt the input payload. Figure 5 and 4 presents the key sensitivity values corresponding to 1000 randomly generated secret keys. The presented results prove that the key sensitivity value is always close to 50% by using the produced dynamic network or application keys. Indeed, the sensitivity of the dynamic secret key DSK is calculated as follows:

$$KS = \frac{\sum_{k=1}^{T} dec2bin(E_{DSK}(P)) \oplus dec2bin(E_{DSK'}(P))}{T} \quad (3)$$

where all the elements of DSK are equal to those of DSK', except for the Least Significant Bit (LSB) of a random byte, and T is the length of the secret keys (in bits).

This result proves that the proposed countermeasure reaches a high level of key sensitivity, since the obtained results are very close to the desired value, which is 50%. Therefore, the proposed update scheme confirms its security since the required sensitivity is attained.

6.2 Countermeasure Crypt-analysis

In this section, the robustness of the proposed countermeasure scheme against the listed attacks is discussed and analyzed. These attacks include replay and eavesdropping attacks. The proposed scheme is considered public and the crypt-analyst is assumed to have complete knowledge regarding all required steps, but none regarding the network and application secret keys.

The proposed solution introduces the dynamicity by updating the network and application keys for each new reset. In addition, the produced dynamic network and server keys are produced by mixing the static ones with the reset counter number or channel parameters for LoRaWAN EDs of class A and B. This means new key stream is produced, since dynamic application key is used. This prevents confidentiality attacks to recover any useful information about the future messages. In parallel, a new dynamic network key will be used, which makes previous messages of previous sessions invalid during the current session. Therefore, the proposed dynamic key derivation technique will prevent replay and confidentiality attacks, since AES meets the message and key avalanche effect. In addition, a secure hash function operation such as SHA-512(one way function) is introduced in the proposed solution for LoRaWAN EDs of class C (high traffic). In fact, the hash function is applied on the output of the mixed secret key with the reset counter. This will make the produced dynamic keys different compared to the static and the previous dynamic ones. In fact, the proposed key derivation scheme presents high collision resistance, where any slight modification in any input produces different network and application keys. Moreover, the size of the counter session is flexible and it can be at least equals to 128 bits.

7 PERFORMANCE ANALYSIS

In this section, the performance of the proposed scheme is assessed in terms of computational complexity, execution time, communication overhead, efficiency, transparency, and flexibility.

7.1 Computational Complexity

In this paper, the proposed solution depends on one or two simple operations, mainly exclusive or (XOR) and/or secure cryptographic hash function. As a result, the computational complexity of the proposed countermeasure is relatively low. The computational complexity overhead is defined as the sum of processing overhead in each update network and application key update process

1. C_{xor} is the overhead of the logical exclusive or (XOR),
2. C_{hash} is the overhead of one hash operation,

The overhead delay of the proposed update mechanism for class A and B EDs is:

$$C_{prop(A,B)} = 2 \times C_{xor} \tag{4}$$

The overhead delay depends of the number of packets transmitted between two ED resets. Low overhead delay is introduced for a big number of packets transmitted between two resets. Therefore, it is clear that the required delay overhead in this solution is low since the proposed scheme requires a lower number of operations. While the required overhead delay for class C EDs is;

$$C_{prop} = 2 \times C_{hash} + 2 \times C_{XOR} \tag{5}$$

$$= C_{prop(A,B)} + 2 \times C_{hash} \tag{6}$$

Here, it is clear that the overhead of the proposed solution for class C EDs is higher compared to class A and B EDs, since it requires two hash operations for each reset. In terms of energy, the EDs of class C are not power constrained, while in terms of delay, it depends on their application. Let us indicate that this cost can be acceptable if a high level of security is necessary.

7.2 Communication Overhead

The proposed solution does not introduce any communication overhead and the reset counter is updated at the EDs. Then, network and application servers received this information from the EDs and consequently update the corresponding counter in the case of the first variant or receive the channel parameters from the GW in the case of the second variant.

8 CONCLUSION

LoRaWAN has appeared in the last few years as an efficient communication technology for IoT applications. However, LoRaWAN suffers from many security vulnerabilities and threats, which lead to attacks against the system confidentiality, integrity, authentication and availability, in addition to privacy issues. In this paper, the proposed solution is based on a new dynamic key derivation approach that updates the network and application keys after each reset operation for ABP end-devices. Therefore, dynamic confidentiality and authentication keys are used for each reset session instead of the static ones, as in the traditional ABP operation mode. Moreover, the proposed countermeasure is adapted to EDS of classes (A,B, and C). Therefore, it is designed to reach a good balance between security and system performance. As a result, the performed security and performance tests validate the efficiency and robustness of the proposed solution. Note that the proposed scheme can be applied also for updating the OTAA root keys (the root key for network server *NwkKey* and the root key for application server *AppKey*) used for deriving the dynamic session keys.

REFERENCES

Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W., and Hughes, D. (2017). Selective jamming of lorawan using commodity hardware. *arXiv preprint arXiv:1712.02141*.

Augustin, A., Yi, J., Clausen, T., and Townsley, W. M. (2016). A study of lora: Long range & low power networks for the internet of things. *Sensors*, 16(9):1466.

Eldefrawy, M., Butun, I., Pereira, N., and Gidlund, M. (2019). Formal security analysis of lorawan. *Computer Networks*, 148:328 – 339.

Han, J. and Wang, J. (2018). An enhanced key management scheme for lorawan. *Cryptography*, 2(4).

Kim, J. and Song, J. (2017a). A dual key-based activation scheme for secure lorawan. *Wireless Communications and Mobile Computing*, 2017.

Kim, J. and Song, J. (2017b). A simple and efficient replay attack prevention scheme for lorawan. In *Proceedings of the 2017 the 7th International Conference on Communication and Network Security*, ICCNS 2017, pages 32–36, New York, NY, USA. ACM.

Kuipers, F. Security vulnerabilities in lorawan.

Lee, J., Hwang, D., Park, J., and Kim, K.-H. (2017). Risk analysis and countermeasure for bit-flipping attack in lorawan. In *Information Networking (ICOIN), 2017 International Conference on*, pages 549–551. IEEE.

Mundt, T., Gladisch, A., Rietschel, S., Bauer, J., Goltz, J., and Wiedenmann, S. (2018). General security considerations of lorawan version 1.1 infrastructures. In *Proceedings of the 16th ACM International Symposium on Mobility Management and Wireless Access*, MobiWac'18, pages 118–123, New York, NY, USA. ACM.

Na, S., Hwang, D., Shin, W., and Kim, K.-H. (2017). Scenario and countermeasure for replay attack using join request messages in lorawan. In *Information Networking (ICOIN), 2017 International Conference on*, pages 718–720. IEEE.

Naoui, S., Elhdhili, M. E., and Saidane, L. A. (2016). Enhancing the security of the iot lorawan architecture. In *Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), International Conference on*, pages 1–7. IEEE.

Noura, H., Chehab, A., and Couturier, R. (2019a). Lightweight dynamic key-dependent and flexible cipher scheme for iot devices. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–8. IEEE.

Noura, H. N., Melki, R., Chehab, A., and Mansour, M. M. (2018). A physical encryption scheme for low-power wireless m2m devices: a dynamic key approach. *Mobile Networks and Applications*, pages 1–17.

Noura, H. N., Melki, R., Chehab, A., and Mansour, M. M. (2019b). A physical encryption scheme for low-power wireless m2m devices: a dynamic key approach. *Mobile Networks and Applications*, 24(2):447–463.

Noura, H. N., Melki, R., Malli, M., and Chehab, A. (2019c). Design and realization of efficient & secure multihomed systems based on random linear network coding. *Computer Networks*, 163:106886.

Ruotsalainen, H. and Grebeniuk, S. (2018). Towards wireless secret key agreement with lora physical layer. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, pages 23:1–23:6, New York, NY, USA. ACM.

Salinesi, C., Mazo, R., Djebbi, O., Diaz, D., and Lora-Michiels, A. (2011). Constraints: The core of product line engineering. In *Research Challenges in Information Science (RCIS), 2011 Fifth International Conference on*, pages 1–10. IEEE.

Salman, O., Elhajj, I., Chehab, A., and Kayssi, A. (2018). Iot survey: An sdn and fog computing perspective. *Computer Networks*, 143:221 – 246.

Salman, O., Elhajj, I., Kayssi, A., and Chehab, A. (2015). Edge computing enabling the internet of things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 603–608. IEEE.

Salman, O., Kayssi, A., Chehab, A., and Elhajj, I. (2017). Multi-level security for the 5g/iot ubiquitous network. In *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 188–193. IEEE.

Sanchez-Iborra, R., Sánchez-Gómez, J., Pérez, S., Fernández, P. J., Santa, J., Hernández-Ramos, J. L., and Skarmeta, A. F. (2018). Enhancing lorawan security through a lightweight and authenticated key management approach. *Sensors*, 18(6).

Sisinni, E., Carvalho, D. F., Ferrari, P., Flammini, A., Silva, D. R. C., and Da Silva, I. M. (2018). Enhanced flexible lorawan node for industrial iot. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, pages 1–4. IEEE.

Sung, W., Ahn, H., Kim, J., and Choi, S. (2018). Protecting end-device from replay attack on lorawan. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pages 167–171.

Tomasin, S., Zulian, S., and Vangelista, L. (2017). Security analysis of lorawan join procedure for internet of things networks. In *Wireless Communications and Networking Conference Workshops (WCNCW), 2017 IEEE*, pages 1–6. IEEE.

Tsai, K.-L., Huang, Y.-L., Leu, F.-Y., You, I., Huang, Y.-L., and Tsai, C.-H. (2018). Aes-128 based secure low power communication for lorawan iot environments. *IEEE Access*, 6:45325–45334.

Vangelista, L., Zanella, A., and Zorzi, M. (2015). Long-range iot technologies: The dawn of lora™ . In Atanasovski, V. and Leon-Garcia, A., editors, *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, pages 51–58, Cham. Springer International Publishing.

Verma, S., Kawamoto, Y., Fadlullah, Z. M., Nishiyama, H., and Kato, N. (2017). A survey on network methodologies for real-time analytics of massive iot data and open research issues. *IEEE Communications Surveys & Tutorials*, 19(3):1457–1477.

Xia, Z., Zhou, H., Gu, K., Yin, B., Zeng, Y., and Xu, M. (2018). Secure session key management scheme for meter-reading system based on lora technology. *IEEE Access*, 6:75015–75024.

Xu, W., Jha, S., and Hu, W. (2018). Exploring the feasibility of physical layer key generation for lorawan. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 231–236.

Xu, W., Jha, S., and Hu, W. (2019). Lora-key: Secure key generation system for lora-based network. *IEEE Internet of Things Journal*, pages 1–1.

Yang, X., Karampatzakis, E., Doerr, C., and Kuipers, F. (2018). Security vulnerabilities in lorawan. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 129–140. IEEE.

Zhang, J., Marshall, A., and Hanzo, L. (2018). Channel-envelope differencing eliminates secret key correlation: Lora-based key generation in low power wide area networks. *IEEE Transactions on Vehicular Technology*, 67(12):12462–12466.