Cybersecurity of the Low Power Wide Area Networks (LPWAN)

Valeria Loscrì, Emilie Bout

Cybersecurity of the Low Power Wide Area Networks (LPWAN)

Main English Title

Bout Emilie

Inria Lille Nord-Europe

emilie.bout@inria.fr

Loscri Valeria

Inria Lille Nord-Europe

valeria.loscri@inria.fr

Synonyms

Cyber attacks in wireless IoT systems

Definition

Cyber-security of LPWAN is the analysis of vulnerability and potential threats for resource-constrained wireless connected objects. It also encompasses countermeasure approaches based on the identified vulnerabilities, that need to meet the computational and energy constraints.

Background

The growing popularity in recent years of the Internet of Things (IoT) and Machine-to-Machine (M2M) communications has fostered the development of major innovations in different sectors. However, the specifications and the constraints related to these new use cases have highlighted three major problems : the guarantee of low power consumption, a wide range, and a high data transmission rate. To respond to these constraints, a new class of wireless networks called Low Power Wide Area Network (LPWAN) has been created and regrouped several types of protocols such as : SigFox, NB-IoT or LoRaWAN. This new type of protocol is characterised with specific features (e.g., duty-cycle approaches to reduce the energy consumption), which can be seen by an attacker as new vulnerabilities.

Theory

Security in LPWAN has been a concern for several years due to their user resource limitations. Indeed, three main attack vectors can be cited : their energy, their management key, and their gateway.
When **energy** is the attack vector, we speak of a subclass of attack called Energy Depletion Attacks. As their name suggests, this type of attack aims to completely drain the energy of a device with unexpected/illegal operation. To cause additional energy expenditure, the attacker has two main alternatives. The first is to provoke an energy cost overhead by forcing the victim to perform additional actions. In this category, we find all the denial of service (DOS) attacks in basic wireless protocols, such as jamming or replay attacks. Indeed, during a jamming attack, the attacker occupies a transmission channel to force the victim to delay its transmission and to remain active during this time. With a replay attack, the receiving node has to process an extra packet, and therefore it will consume more power than expected. In [1], the authors discuss the energy consumption of a LoraWan network when it undergoes a jamming attack. They demonstrate that the attack increased the total power consumption of a single communication event from 36% to 576%. The second alternative for the attacker is to play with the different paradigms put in place to save energy in the LPWAN protocol. This type of category includes more targeted and elaborate attacks. Indeed, in recent years attackers have begun to integrate

intelligent actions into their process to better respond to the specificities of victim protocols and make decisions autonomously. In [2], the authors develop a new attack based on an energy-saving mechanism, the duty-cycle. With a process of Markov chain theory, the authors demonstrate that thanks to the duty cycle mechanism, it is possible to deduce the optimal moment of the attack. They reveal that this type of attack considerably reduces network performance and causes numerous retransmissions which affect energy consumption.
The second attack vector is the **key management**. Indeed, to ensure the integrity and confidentiality of data, the notion of session key has been integrated into the LPWAN protocols. For example, the LoraWan protocol includes two 128-bit pre-shared root keys stored in memory to derive the session key and ensures the integrity of payload data on the MAC layer. Thus, each device has a specific signature. However, like any new method of ensuring security, these can also become new targets or allow the inference of information. Indeed, most of the time these keys are directly stored in the memory of the device and are not re-initiated after their manufacture. Additionally, the encryption key and method no longer change once devices are deployed in most cases. Indeed, designing encryption algorithms that evolve over time and consume little energy is still an open research topic and few solutions have been integrated into reality. Therefore, if an attacker has the same type of device, he can easily deduce the encryption algorithm as well as the key. Moreover, an attacker having physical access to a node, can extract the key and decrypt the communication.
The last attack vector on this type of network is **the gateway**. Indeed, the gateway component is an important part of the LPWAN network to ensure connectivity with end devices. However, this type of device contains valuable endpoint and management security information such as keys. An attacker can target the gateway to gain access to this information to later create other types of attacks such as spoofing attacks. Moreover, since the main purpose of this device is to provide connectivity between network nodes, this latter represents a single failure point for the network which could be used to disconnect hundreds of end-device from application. Finally, secret keys can also be deduced with a side channel attack. By analyzing the behavior of the embedded device such as the USIM cards on the gateway, the attacker is able to discover personal information. Indeed, in [3], the authors based on a Differential Power Analysis, deduce the secret key present in the gateway.

Future directions

Securing LPWAN networks remains an important issue and an open research topic. One of the first possible improvements would be the implementation of a system to reduce the energy consumption of more robust networks. A useful goal would be to create a system capable of detecting any type of attack underway and react appropriately. In this type of idea, several intrusion detection systems (IDS) have been developed in the literature [4]. However, problems such as the placement of the IDS solution in the network still remains to be resolved. Indeed, as we pointed out just above, if the IDS is installed directly in the gateway but it is corrupted, the latter will become ineffective. In order to respond to the security problem linked to the management key, several works are also in progress, as in [5]. In this work, the authors implement a novel low-power AES data encryption architecture to reduce power consumption and increase session key renewal security. More work has been done in this direction in recent years, however, as with IDS, there are still general points to be answered. For example, this new work improves the power consumption of the key generation and exchange process but significantly reduces the performance and data transmission rate of the devices. More generally, the improvement of security in recent years has gone through the creation of attacks. Many solutions to increase LPWAN networks have been integrated into the protocols. However, security has rarely been studied during their creation or integration. Recently, attacks targeting these systems have taken place, these are adversary attacks aimed at compromising security systems based on machine learning algorithms [6].

References

[1] Konstantin Mikhaylov et al. “Energy Attack in LoRaWAN : Experimental Validation”. In : *Proceedings of the 14th International Conference on Availability, Reliability and Security*. ARES ’19. Canterbury, CA, United Kingdom : Association for Computing Machinery, 2019. isbn : 9781450371643. doi : 10.1145/3339252.3340525.

[2] Emilie Bout, Valeria Loscri et Antoine Gallais. “HARPAGON : An energy management framework for attacks in IoT networks”. In : *IEEE Internet of Things Journal* (2022), p. 1-1. doi : 10.1109/JIOT.2022.3172849.

[3] Junrong Liu et al. “Small Tweaks Do Not Help : Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards”. In : *Computer Security – ESORICS 2015*. Sous la dir. de Günther Pernul, Peter Y A Ryan et Edgar Weippl. Cham : Springer International Publishing, 2015, p. 468-480. isbn : 978-3-319-24174-6.

[4] Mohamed Faisal Elrawy, Ali Ismail Awad et Hesham FA Hamed. “Intrusion detection systems for IoT-based smart environments : a survey”. In : *Journal of Cloud Computing* 7.1 (2018), p. 1-20.

[5] Kun-Lin Tsai et al. “Low-Power AES Data Encryption Architecture for a LoRaWAN”. In : *IEEE Access* 7 (2019), p. 146348-146357. doi : 10.1109/ACCESS.2019.2941972.

[6] Yashar Deldjoo, Tommaso Di Noia et Felice Antonio Merra. “A Survey on Adversarial Recommender Systems : From Attack/Defense Strategies to Generative Adversarial Networks”. In : *ACM Comput. Surv.* 54.2 (mars 2021). issn : 0360-0300. doi : 10.1145/3439729. url : https://doi.org/10.1145/3439729.