Analysis of LoRaWAN and NB-IoT for Critical and Massive Communication

Mateo Campoverde-Fordon[1][0009−0006−4806−4945] and
Birger Andersen[2][0000−0003−1402−0355]

[1] University of Illinois Urbana-Champaign, Champaign, IL, 61801, USA
mateojc2@illinois.edu
[2] Technical University of Denmark, Copenhagen, Denmark
birad@dtu.dk

Abstract. LoRaWAN and Narrow-Band Internet-of-Things (NB-IoT) are gaining popularity for communicating data through low-cost, long-range, and compact devices. The applications for these low-power wide area network (LPWAN) devices are expansive, as these devices can monitor large systems without the inconvenience of physical wires for data transmission. This opens possibilities for gathering data in difficult and/or dangerous environments. However, as data is being sent wirelessly, devices are prone to wireless attacks. In this analysis, we rank LoRaWAN and NB-IoT in terms of practicality and security concerns. Specifically, we analyse the physical devices and the wireless communication to their respective gateways. We also explain how attacks such as jamming, bit-flipping, and SIM swapping affect massive and critical IoT scenarios. Our analysis shows that NB-IoT is preferable for critical communication, whereas LoRaWAN is an attractive choice for massive communication scenarios.

Keywords: NB-IoT · LoRaWAN · LPWAN · Massive IoT · Critical IoT · Eavesdropping · Bitflipping · Jamming · DevEUI Catching · SIM Swapping · Replay Attack · ISMI Catching · Soft Downgrade Attack

1 Introduction

As wireless devices are becoming more compact, powerful and low-cost, new ways of collecting data are available for large systems. LoRaWAN, NB-IoT, LTE-M and Sigfox are LPWANs that enable easy monitoring of systems with many parts. This analysis will cover pervasive threats for LoRaWAN and NB-IoT devices, as well as proposed use cases for both.

We will focus at LoRaWAN and NB-IoT because of their growing popularity compared to other LPWANS. It is projected that LPWANS will have a 50% growth rate by 2034 in applications such as transportation, healthcare and manufacturing [1].

Ericsson [2] loosely categorizes IoT devices as either being used in massive or critical applications. In critical applications such as traffic control and healthcare,

wireless devices should provide quick and reliable data. In massive applications such as agriculture, smart buildings, and metering, larger amounts of smaller data should be collected through many IoT devices, whereas quick and reliable data delivery does not have quite the same role.

In this analysis we will consider LoRaWAN and NB-IoT for use in massive and critical IoT. We will categorize the technologies by their practicality and list their security concerns by severity.

2 Related Work

There are several articles that cover both the security features and flaws of LoRaWAN, NB-IoT and other WPLAN technologies. [3, 4] describe security threats to LoRaWAN from the device itself to possible flaws in the user facing application. These articles have been used for researching current vulnerabilities in LoRaWAN such as replay attacks. Articles such as [5, 8] are more specific in the type of attacks regarding LoRaWAN. These articles discuss jamming and bitflipping techniques, and provide remedies that could be implemented in the future. Likewise, there are articles [9, 10] that can be found for specific NB-IoT attacks such as ISMI catching and jamming. There are also articles that cover vulnerabilities for LPWANS that include NB-IoT and LoRaWAN such as [11, 12]. These articles help for general overviews of the WPLAN landscape, and which LPWANs would fit the application at hand.

This paper provides the theory and practicality toward NB-IoT and LoRaWAN v1.1 attacks. In our analysis, we have compiled and ranked critical vulnerabilities and security concerns for both technologies. We also express our concerns and recommendations for both LPWANS in the monitoring of massive and critical IoT systems.

3 LoRaWAN

LoRaWAN is an open protocol to create long-range networks through the use of LoRa, a proprietary radio communication scheme. Maintained by The LoRa Alliance, LoRaWAN can be used in many data collection applications. As LoRa devices are deployed in a star topology, LoRaWAN is used to communicate between end devices and LoRa gateways before data is relayed to application servers [13].

3.1 Practicality

LoRa devices are low-cost, battery-operated and compact which allow for large network deployments. As LoRa devices are not dependent on any preexisting network infrastructure, relatively inexpensive LoRaWAN gateways must be purchased to capture LoRa packets. Up to 10,000 devices can be managed by a single gateway [14] and a signal sent to many gateways will be received by the

network server. Here duplicates are removed and a single message is forwarded to application server. The range of a single LoRa device roughly is 10km, although data can be relayed through gateways. Device mobility is supported as long as gateways connected to same network server are within range. Radio bands are unlicensed and therefore anyone can setup an own network with gateways and servers, although it is more simple to connect gateways to existing servers such as The Things Network (TTN). However, this also means that radio interference can be expected.

3.2 Security

There are two ways to deploy a LoRa v1.1 device to a network: Over-The-Air-Activation (OTAA) and Activation-By-Personalization (ABP).

Devices using OTAA join a network through a key generation handshake, creating unique keys for each session. Before joining, each device must store an unique device identifier (DevEUI), join server identifier (JoinEUI), application root key (Appkey) and a network root key (NwkKey). As seen in Fig. 1, LoRa devices send a Join-Request with a message integrity code (MIC, calculated with NwkKey) which is then relayed by the gateway to the Join-Server. After the Join-Server verifies the request, it generates session keys for the network server (NwkSKey), application server (AppSKey), and device (FNwkSIntKey, SNwkSIntKey, NwkSEncKey). Then the network session key (NwkSKey) and app session key (AppSKey) are distributed to the network server and app session respectively. Lastly, an Advanced Encryption Standard (AES, Fig. 3) encrypted Join-Accept message is sent to the device [15]. The end device is able to produce AppSKey, FNwkSIntKey (Forwarding network session integrity key), SNwkSIntKey (Serving network session integrity key) and NwkSEncKey (Network session encryption key) independently as the handshake shares nonces which are used to calculate said keys. The key hierarchy is displayed in Fig. 2.

End devices using ABP will have the FNwkSIntKey, SNwkSIntKey, NwkSEncKey and AppSKey stored directly to the device, circumventing any key generation handshake. In the event of manufacturers or end users using the same keys and identifiers for multiple devices, LoRaWAN gateways will be unable to distinguish incoming packets from different devices.

For end devices sending messages to the application server, all packet data is encrypted using AppSKey. This ensures end-to-end encryption from the device to the end user application. Additionally, LoRa packets include a counter value that is checked by the LoRa gateway used to ensure packets are not lost in transmission. If a packet's counter is less than (or greater than a configurable margin of error) the LoRa gateway's stored counter, it will be dropped.

1. Eavesdropping This attack is applicable to devices using ABP v1.1, as encryption keys do not change. To eavesdrop on LoRa packets, two packets must be captured with the same counter value. As AES Counter mode (CTR, Fig. 3) is used for encryption, XORing two encrypted payloads (C_1, C_2) using private

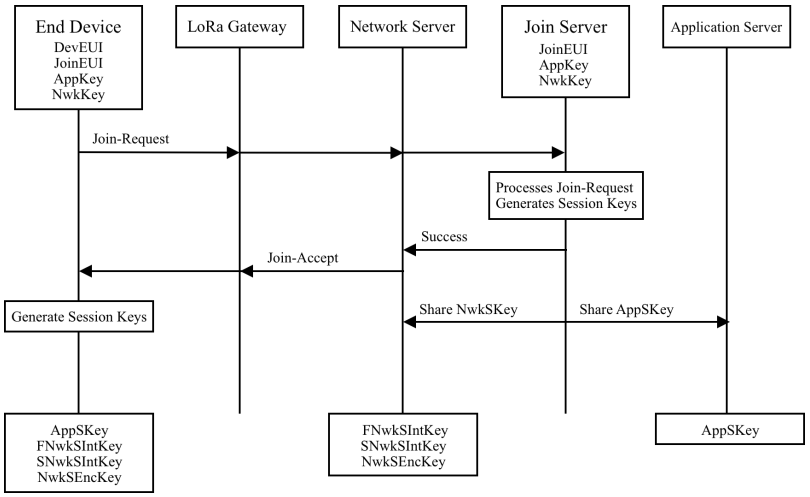

Fig. 1. OTAA for LoRaWAN v1.1 [15]

$$AppSKey = aes128_{encrypt}(AppKey, 0x02|JoinNonce|JoinEUI|DeviceNonce|pad16)$$

$$FNwkSIntKey = aes128_{encrypt}(NwkKey, 0x01|JoinNonce|JoinEUI|DeviceNonce|pad16)$$
$$SNwkSIntKey = aes128_{encrypt}(NwkKey, 0x03|JoinNonce|JoinEUI|DeviceNonce|pad16)$$
$$NwkSEncKey = aes128_{encrypt}(NwkKey, 0x04|JoinNonce|JoinEUI|DeviceNonce|pad16)$$

Fig. 2. LoRaWAN Key Hierarchy [13]

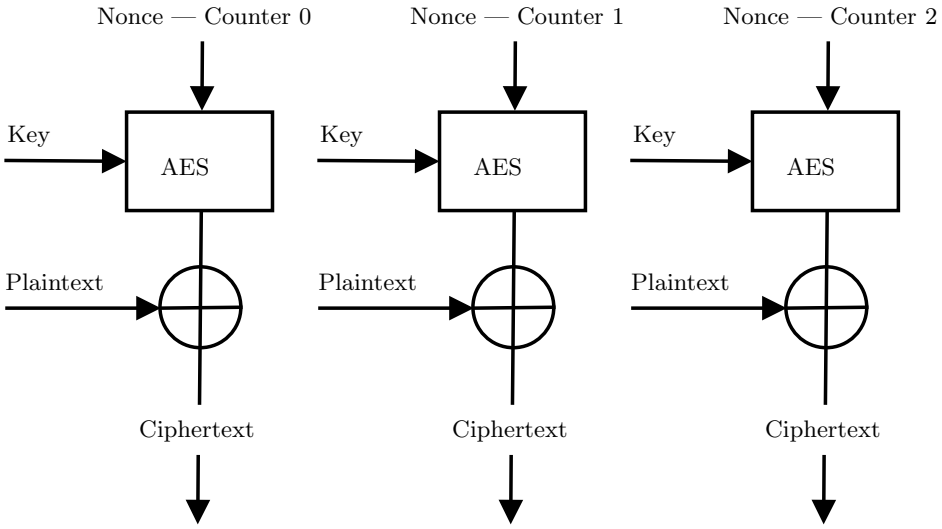

Fig. 3. AES CTR Mode

key K would yield the XOR of the plaintext data (P_1, P_2). This is shown in Fig. 4.

$$\begin{aligned} C_1 \oplus C_2 &= (P_1 \oplus K) \oplus (P_2 \oplus K) \\ &= (P_1 \oplus P_2) \oplus \cancel{(K \oplus K)} \\ &= P_1 \oplus P_2 \end{aligned}$$

Fig. 4. Plaintext Retrieval

From here, crib dragging techniques can be used to retrieve each plaintext. As LoRaWAN devices are expected to transmit data sparingly, this attack will likely take years to capture packets with the same counter value. However, if multiple LoRa devices using ABP have identical session keys, then more packets could be captured which could lead to a faster counter matching. This is the most severe vulnerability for devices using ABP as it can exploited remotely and retrieve any sensitive data in transit. The confidentiality of a LoRaWAN device could be compromised with this exploit [3, 4].

2. Jamming It is easy and inexpensive to jam LoRa gateways with Gaussian noise. It has been shown using a low-cost ESP32 with a LoRa attachment that LoRa gateways fail to receive any packets from LoRa devices. More intelligent jammers can selectively choose when to release noise, increasing their power efficiency and making them harder to detect. Utilizing LoRa's Adaptive Data Rate feature can help defend against these attacks, although it requires more power, shortening the lifespan of the device. Jamming is common across all radio communication technologies as it is easy to achieve. While not as nosy as eavesdropping, jamming is an attack on availability as all valuable data is lost to noise [5]. A LoRaWAN device only re-transmits its data if the device software application includes such feature. Jamming will be difficult to detect since radio band is unlicensed and interference from other traffic is normal.

3. DevEUI Catching As mentioned earlier, DevEUIs are used for identifying individual LoRaWAN devices. DevEUIs are exposed during OTAA Join-Request and Rejoin-Request packets within the frame header. If an attacker were to capture LoRa packets with DevEUI information, the attacker could track the rough location of the LoRa device [6]. If an attacker jams a LoRa device to force a Rejoin-Request, then the DevEUI could be captured again. When joining, a device is assigned a 32-bit device address which is uses until a rejoin. This address may be caught as well. DevEUI catching (or address catching) is a breach of privacy as the location of a LoRaWAN device could be disclosed and used for physical attacks. However, DevEUI catching is not very practical as LoRaWAN devices are physically small and this vulnerability gives an approximation of

a device's location. Although if a device is captured, then ABP keys may be extracted allowing for more serious LoRaWAN attacks. If device is carried by a person, it will allow for tracking of the person.

4. Replay Attack In addition to jamming LoRa devices, packets from LoRa devices using ABP can be captured and released on command. This works as packets are not timestamped and ABP is not dependent on dynamic session keys [7]. However, an attacker must wait until the counter value FCnt overflows to the first captured counter value, so that captured messages can be repeated. It should be noted that a configurable margin of error can exist for counter values, such that FCnt values can skip ahead causing packets with lower counter values to be discarded. By releasing increased counter packets within this gap, any legitimate packets of a lower counter value will be discarded by the LoRa gateway. This attack could be a greater breach of integrity if LoRaWAN packets were not sent as infrequently. Because of the delay between packets being sent, it may take years for a replay attack to be viable. At that point, the LoRaWAN device may have reached the end of its lifecycle.

5. Bit-flipping Bit-flipping is a concern for LoRaWAN as the integrity of packets can be compromised, but still appear authentic. Although LoRaWAN uses AES CTR mode to encrypt packet payloads, the position of the data bits are not shuffled (Fig. 3). This means if the structure of the plaintext data is known, specific bits could be targeted. To falsify authenticity after modifying the data, all MIC combinations can be brute-forced within 1516.5 milliseconds using a quad-core processor [8]. Due to the amount of forged MIC possibilities, it is unlikely that a forged LoRaWAN packet would be accepted. Considering on average 2,147,483,648 attempts are needed before a valid MIC is forged, an authentic packet may be transmitted before the modified packet. This means the new authentic packet would carry an incremented frame counter, and the modified packet would be invalid regardless of MIC value [4].

6. Backward Compatibility Vulnerabilities In the event a LoRaWAN v1.1 device and a v1.0.2 back-end are communicating or vice versa, there are attacks vulnerabilities that could be exploited. Although LoRaWAN v1.1 addresses issues such as replay, eavesdropping, ACK spoofing, and DoS attacks, these attacks are reinstated when a LoRaWAN network is configured with mismatching software versions [16]. This is due to the sacrifice of keys and message types when a LoRaWAN device or back-end has v1.0.2.

4 NB-IoT

Narrow-Band Internet of Things (NB-IoT) is a LPWAN technology standardized by the 3rd-Generation Partnership Project (3GPP). Using long-term evolution (LTE) technology, NB-IoT utilizes preexisting cellular infrastructure to transmit data. Because of this, NB-IoT requires subscriber identity module (SIM) cards to function on mobile carriers.

4.1 Practicality

As NB-IoT utilizes preexisting cellular infrastructures as 4G and 5G maintained by mobile carriers to transmit data, no gateways need to be purchased. This greatly increases the operating range of NB-IoT devices as mobile carriers have high global coverage. Device mobility is therefore supported. Mobile carriers operate in licensed bands and have thus full control of traffic, so no interference from unknown traffic is expected.

4.2 Security

NB-IoT is based of LTE security and uses SIM cards for secure communication. Because of this, NB-IoT devices have security features that are used in more popular and expensive devices, such as smartphones. Additionally, many cellular optimizations can be used to transfer data securely such as Non-IP Data Delivery (NIDD) and Data Over Network Attached Storage (DoNAS) [17].

1. SIM Swapping If an attacker were to locate a NB-IoT device and retrieve its SIM card, a SIM swapping attack could take place. By swapping the SIM card to a malicious device, the attacker may be able to connect to the Packet Data Network Gateway (PGW) that hosts the private LAN for the legitimate NB-IoT devices. As NB-IoT devices are capable to send IP data, the malicious device may detect open ports and perform common IP attacks. By gaining access to the private LAN, a malicious device could also deplete resources of legitimate devices. By flooding any devices with open ports with spoofed traffic on the network, devices expend their batteries resulting in a denial of service (DoS). SIM swapping can almost be prevented with the use of embedded SIM cards (eSIMs). As eSIMs are soldered directly to the NB-IoT device, it would be difficult to remove the eSIM without damaging it. This is the biggest threat to NB-IoT devices as an attacker can gain direct access to the PGW for other NB-IoT devices. If additional IP vulnerabilities are found on open ports of NB-IoT devices, then not only integrity, but confidentiality and availability may be compromised [11].

2. Soft Downgrade While NB-IoT was designed with 4G in mind, manufacturers are still producing NB-IoT chipsets with 2G fallback. This means if an attacker is able to spoof TAU reject messages and force the device to connect using a malicious 2G base station, a man-in-the-middle attack could take place. In the event of new vulnerabilities regarding cellular communication, NB-IoT devices will be affected as they are dependent on cellular infrastructure and protocols.

Because of how this attack would intercept any packets in transit, their contents could be observed or even modified. If successful, this attack could be very powerful at gathering data from NB-IoT devices and would compromise confidentiality and integrity. However, NB-IoT devices may be physically or digitally configured to prevent fallback, meaning this attack would not work [18].

3. IMSI Catching All SIM cards are assigned an international mobile subscriber identity (IMSI), which means NB-IoT devices can be uniquely identified and tracked by an attacker. IMSI Catchers can be used to impersonate a LTE network in order for NB-IoT and other cellular devices to expose their IMSI. This is because Tracking Area Update (TAU) reject messages can be spoofed, resulting in a cellular device to give up their IMSI through a reactive Attach Request message. Autonomous IMSI catchers have been made through the use of software defined radios (SDRs), Low Noise Amplifiers (LNAs), Raspberry Pis, and open-source software. Although IMSI catchers are relatively small and easy to hide, SDRs are expensive and can limit the practicality of this attack. From gathering a device's IMSI, an attacker can locate the NB-IoT device and perform physical attacks on the device. This is an attack on privacy of owner carrying device and availability as a NB-IoT device can be located and possibility destroyed on discovery [12, 9].

4. Jamming NB-IoT operates within licensed, regulated spectrum bands meaning interference from other radio technologies are kept to a minimum. However, as with other radio communication technologies, NB-IoT devices are still susceptible to jamming attacks. Jammers that produce noise at the operating frequency channel of NB-IoT devices can cause packet loss. However, as cellular infrastructure is maintained by the network operators, it is likely that jamming attacks would alert authorities. Likewise, network operators likely have more frequency channels available for NB-IoT devices to be assigned and reconnect to. Successful jamming affects the availability of NB-IoT devices as it disrupts communication from the device.

5 Discussion

Table 1. Overview of Major Threats

Threat	LoRaWAN	NB-IoT
Confidentiality	Eavesdropping	SIM Swapping Soft Downgrade
Availablility	Jamming	Jamming Soft Downgrade
Privacy	DevEUI Catching	ISMI Catching
Integrity	Bitflipping Replay Attack	SIM Swapping Soft Downgrade

As listed by order of severity earlier, there are many vulnerabilities that affect both LoRaWAN and NB-IoT. One can see that both technologies have a comparable amount of security concerns.

In Table 1. are the discussed security concerns for NB-IoT and LoRaWAN. Each security concern is categorized under confidentiality, integrity, availability, and privacy for comparison purposes.

Our findings are consistent with other articles, such that both LoRaWAN and NB-IoT have vulnerabilities that exist in their most recent updates. However,

NB-IoT's concerns are considerably more difficult to perform. At the same time, LoRaWAN has more serious issues regarding confidentiality and integrity. This is due to several factors, as LoRaWAN is a newer technology and does not have the same scope of expertise as 3GPP does when developing NB-IoT.

IoT device applications can be broadly categorized as either critical or massive. Massive IoT is used to gather smaller amounts of data at a large scale while critical IoT must communicate data quickly and reliably.

From our investigation on how NB-IoT utilizes LTE security and consequentially has fewer security concerns, NB-IoT is a better candidate for healthcare, traffic control, and other critical IoT applications. SIM Swapping and Soft Downgrade attacks require great effort that can largely be prevented by eSIMs and strict 4G usage. On the other-hand, we have shown how LoRaWAN may be more practical for monitoring massive static systems that have little cellular reception. The severity of ABP attacks make LoRaWAN an easy target for attackers which is why LoRaWAN should be used for less critical applications. ABP should thus be avoided and OTAA used instead.

6 Conclusion

In this analysis we have covered various security concerns and features regarding LoRaWAN and NB-IoT. We have also shown the practicality for implementing these theoretical attacks as different hardware is needed for both LPWANs. Both technologies have a comparable amount of security flaws, although the flaws in LoRaWAN are considerably more severe.

LoRaWAN flaws can be exploited cheaply and remotely. On the other hand, to exploit NB-IoT devices expensive equipment (SDRs) is need and in some cases physical access to a device (SIM Swapping). However LoRaWAN could excel in localized applications where large amounts of less sensitive data is being transmitted. As NB-IoT is supported by 3GPP and mobile service providers, more maintenance and reliability can be ensured. For these reasons, NB-IoT should be considered for critical IoT applications such as healthcare, traffic control, etc. Likewise LoRaWAN should be considered for massive IoT applications such as agriculture and metering. Still ABP should be avoided and OTAA used instead.

References

1. Preeti Wadhwani: Low Power Wide Area Network (LPWAN) Market, 2023-2032, https://www.gminsights.com/industry-analysis/low-power-wide-area-network-lpwan-market Last accessed 14 Aug 2023
2. Ericsson White Paper: Cellular networks for massive IoT. Uen 284 23-3278 (2016)
3. X. Yang, E. Karampatzakis, C. Doerr and F. Kuipers: Security Vulnerabilities in LoRaWAN. In: IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 129-140, https://doi.org/10.1109/IoTDI.2018.00022. (2018)
4. Oliveira, Rafael: LoRaWAN v1.1 security survey (2020)

5. Jonas Stenholt Melchior Jensen, Bjørn Alexander Wade Patterson, Tomasz Blaszczyk, Birger Andersen: Jamming LoRa and Evaluation of Ease of Implementation. In: EAI IoECon 2023 - The Second EAI International Conference on the Internet of Everything (2023)
6. Budykho, Boureanu, I. C., Wesemeyer, S., Romero, D., Lewis, M., Rahulan, Y., Rajaona, F. (n.d.): Fine-Grained Trackability in Protocol Executions. 30th Annual Network and Distributed System Security (NDSS) Symposium (2023)
7. T. Perković, J. Šabić, K. Zovko and P. Šolić: An Investigation of a Replay Attack on LoRaWAN Wearable Devices, 2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Dubrovnik, Croatia (2023)
8. JungWoon Lee, DongYeop Hwang, JiHong Park, Ki-Hyung Kim: Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. In: Da Nang, 2017 International Conference on Information Networking (ICOIN), pp. 549-551. https://doi.org/ 10.1109/ICOIN.2017.7899554. (2017)
9. Ivan Palamà, Francesco Gringoli, Giuseppe Bianchi, Nicola Blefari-Melazzi, IMSI Catchers in the wild: A real world 4G/5G assessment. Computer Networks, Volume 194, 108137, ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2021.108137 (2021)
10. K.F. Muteba, K Djouani, T. Olwal: 5G NB-IoT: Design, Considerations, Solutions and Challenges. Procedia Computer Science, Volume 198, Pages 86-93, https://doi.org/10.1016/j.procs.2021.12.214. (2022)
11. Florian Laurentiu Coman, Krzysztof Mateusz Malarski, Martin Nordal Petersen, Sarah Ruepp: Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT (2019)
12. Oriol Solà Campillo: Security Issues in Internet of Things. Universitat Politècnica de Catalunya, Enginyeria de Telecomunicació (2017)
13. LoRaWAN™1.1 Specification, https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 Last accessed. 10 Aug 2023
14. What are LoRa® and LoRaWAN®?, https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/ Last accessed 13 Aug 2023
15. End Device Activation, https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/ Last accessed 13 Aug 2023
16. Tahsin C.M. Dönmez, Ethiopia Nigussie: Security of LoRaWAN v1.1 in Backward Compatibility Scenarios. Procedia Computer Science, Volume 134, Pages 51-58, https://doi.org/10.1016/j.procs.2018.07.143. (2018)
17. Security Features of LTE-M and NB-IoT Networks, https://www.gsma.com/iot/wp-content/uploads/2019/09/Security-Features-of-LTE-M-and-NB-IoT-Networks.pdf. Last accessed 15 Aug 2023
18. ALT1255: NB-IoT with 2G Fallback, https://altair.sony-semicon.com/products/alt1255/ Last accessed 17 Aug 2023