Addressing Security Concerns in IoT: Insights from Communication Engineering

Yueheng Zhang

Beijing-Dublin International College, Beijing University of Technology, Beijing, China
yueheng.zhang@ucdconnect.ie

Abstract. The Internet of Things (IoT), which refers to a combination of devices, systems, and services, is a new concept that goes beyond machine-to-machine communications and contains advanced automation and integrated cyber-physical systems. Communication engineering is the basis of this transformation, providing the fundamental support for device interconnectivity and data exchange. However, the integration of communication technologies within IoT has also brought complex security challenges that must be overcome to provide the integrity, confidentiality, and availability of signals and messages. This essay examines the multiple applications of communication engineering within the IoT, as well as the security issues during its implementation. It commences with an introduction and comparative analysis of various communication protocols that are widely accepted in the IoT ecosystem, analyzing their performance, efficiency, and reliability in data transmission. Subsequently, the essay discussed the security vulnerability of these protocols and the potential threats they brought to IoT networks. With the aim of overcoming these challenges, the essay conducts a comprehensive analysis of security solutions including encompassing encryption technologies, secure communication protocols, and authentication mechanisms.

Keywords: Internet of Things, Communication Engineering, Security Issues, Wireless Communication Protocols, Data Confidentiality.

1 Introduction

1.1 Overview

IoT is recently a fresh concept that usually regarded as an extension of the internet. In the last half-decade, the adoption rate of the IoT has witnessed a meteoric rise, with the number of connected devices worldwide reaching 20.35 billion in 2017, and is predictable that the amount might rise to 75.44 billion by 2025 [1]. By connecting physical objects to the internet via wired or wireless methods, IoT enables seamless communication between devices, a concept often referred to as “machine-to-machine communications” [2]. Four

Y. Yue (ed.), *Proceedings of the 2024 International Conference on Mechanics, Electronics Engineering and Automation (ICMEEA 2024)*, Advances in Engineering Research 240,
https://doi.org/10.2991/978-94-6463-518-8_41

basic components for such technology are considered to be wireless sensor networks (WSNs), radio frequency identification (RFID), machine-to-machine (M2M) communications, and supervisory control and data acquisition (SCADA) [3]. Different protocols are followed by these components to exchange information, realizing functionalities include automatic identification, localization, real-time tracking, monitoring, and management of physical items. The structure of IoT system includes three main layers [4]:

The sensing Layer (Perception) contains various IoT devices equipped with sensors. Numerous of information are collected through these sensors and are transmitted to the application layer or execute corresponding actions based on received instructions.

The network layer, which is responsible for inter-device communication, can form self-organizing networks using lightweight protocols or connect to local area networks. Efficient communication within this layer enhances the quality and speed of information transmission.

The application layer includes the cloud platforms and mobile apps, which provide the functionalities of device integration, service coordination, and voice control. Mobile apps are usually served as user control terminals, displaying device status and executing commands.

1.2 Communication Engineering in IoT

Communication technologies in the IoT primarily encompass two aspects: sensor network communication technologies and telecommunication transmission network technologies [5]. The former is the peripheral networks that mainly use short-range communication technologies, including RFID, NFC, Bluetooth, and ZigBee [6]. The latter, which referred to core carrier networks such as WIFI, WiMAX, which contains interconnect communication technologies between sensor networks and transmission networks as well as the telecommunication network's own communication technologies [5]. These include wired communication technologies like SDH and all-optical networking, along with wireless communication technologies that has progressed through five generations (1G to 5G).

1.3 Security in IoT

As the IoT increasingly integrated into industrial and daily activities, it highlights the security challenges. The rapid expansion of IoT devices surpasses the existing security infrastructures, leaving an environment filled with potential risks [4]. For instance, hackers could remotely compromise implantable medical devices or intelligent transportation systems, which not only potentially cause substantial economic losses but also leads to sever risks to individual and public safety [1]. Moreover, the pervasive integration of IoT devices in sectors critical to society and national security, such as

industrial and military operations. It is also notes that designers and operators of industrial equipment often has a false sense of security, believing that attackers lack the specialized knowledge to conduct cyberattacks [7]. Moreover, these devices are engineered for specific industrial tasks, and their software and hardware architectures are different from those of conventional computers. Standard computer defense measures, such as firewalls and antivirus software, are not directly applicable to these devices, and designing individual defense measures for each type of industrial device is prohibitively expensive.

At present, there is a discernible deficit in the awareness of Internet of Things (IoT) security and privacy measures among nations, corporations, and individuals [8]. A 2016 survey conducted by the Pew Research Center indicates that a majority of users, approximately 52%, are amenable to sharing health data collected by their personal medical devices with healthcare providers, and 44% consent to the acquisition of temperature data from their domiciles by manufacturers through sensors [7]. Concurrently, a predominant belief among manufacturers is that the integration of additional security protocols does not enhance the marketability of devices but rather inflates production costs. This perspective has led to a paucity of post-sale support in terms of updates, and high-risk vulnerabilities remain within IoT devices, such as default passwords and the plaintext transmission of keys. Therefore, developing and applying strong loT-specific security strategies has become a critical priority. This article will focus on the perspective of communication engineering, analyze the security issues encountered by various communication protocols in the practical application of the loT, and propose potential solutions.

2 Communication Protocols

IoT devices, having the limitations of computational resources and the necessity for low-power operation, are necessary to the security frameworks of both enterprises and private households. However, their accessibility also leads to the possibility of malicious entities. Consequently, the design of IoT protocols must prioritize data security without compromising on energy efficiency, ensuring secure inter-entity communication. This section will divide the essential security issues of IoT wireless protocols into three domains including secure pairing processes, data confidentiality and integrity, resistance ability to replay attacks, and signal interference. The security efficacy of several prevalent IoT protocols will be evaluated according to these standards, and possible solutions to address the security facets will also be covered. These protocols contain RFID, Zigbee, and Wi-Fi, which are extensively employed in smart homes and analogous environments, as well as the long-range LoRa protocol, generally utilized in smart cities and agricultural applications.

2.1 RFID

RFID is a contactless automatic identification technology that is composed of three main components: tags, readers, and antennas. Tags store information about objects and are attached to them for identification purposes; readers are responsible for reading information from tags and rewriting data back inside; antennas facilitate signal transmission between tags and readers [5]. RFID is able to both low and high-frequency systems, adapting to various frequencies following ISO/IEC and EPC Global standards. Its advantages include rapid identification, large data storage capacity, long lifespan, and a wide range of applications [9]. The most commonly used protocol in RFID is EPC Gen2. As for its secure Pairing Process, such protocol incorporates specific security mechanisms, for instance, the Access Password, which serves to restrict read and write operations on tags. The transition of tag states necessitates a sequence of legitimate commands, enhancing security by ensuring that tags only respond when in the correct state [10]. In Data Confidentiality and Integrity, the EPC Gen2 standard offers measures for data encryption and authentication to safeguard the security and privacy of tag data. The tag memory is partitioned into four distinct banks: Reserved, EPC, TID, and User, with the Reserved area holding the Kill Password and Access Password, contributing to the protection of data security [11]. As for the resistance to Replay Attacks and Signal Interference, the EPC Gen2 protocol contemplates anti-collision mechanisms, such as dynamically adjusting frame length based on a slotted ALOHA framework, aiding in the reduction of communication conflicts between tags. Despite EPC Gen2 inherently possessing anti-interference capabilities, a dense tag environment may introduce interference issues, where additional security measures to enhance its resistance to interference are necessary.

2.2 Bluetooth

Bluetooth refers to a wireless communication technology, which implement the information exchange between devices within a range of approximately 10 meters, aiming to replace traditional wired connections. It features wirelessness, openness, compatibility, mobility, anti-interference, low power consumption, and low cost [12]. Bluetooth devices transmit radio signals over short distances using dedicated chips, supporting high-speed frequency hopping and short packet technology to reduce interference and ensure reliable transmission. Moreover, operating in the ISM band, Bluetooth offers global universality and supports various transmission distances based on different power levels. Point-to-point or multipoint communication is enabled, which allows multiple devices to exchange information equally within a network. The Bluetooth system consists of antenna units, link control hardware, link management software, and protocols, which was developed by Ericsson in 1994, and later collaborated with IEEE to establish the IEEE802.15.1 standard [9]. As for the secure pairing processes, such protocol aligns with Bluetooth v1.1

specifications and includes the Link Manager Protocol (LMP) that handles the pairing process between devices. This process involves the creation of a shared secret link key that is used for authentication and encryption key generation. Data confidentiality and integrity are maintained in IEEE 802.15.1 through encryption and authentication mechanisms [13]. The protocol supports encryption based on the E0 stream cipher for protecting the payload and a challenge-response scheme for authentication. Fequency hopping spread spectrum (FHSS) is also employed in IEEE 802.15.1 to mitigate signal interference and reduce the risk of interception and replay attacks [14]. The rapid change of frequencies makes it difficult for attackers to track and replay the communication.

2.3 ZigBee

ZigBee constitutes a protocol engineered for low-energy, wireless exchanges, optimized for brief-distance interactions, suitable for periodic or intermittent data transmission. It supports large-scale networks with up to 65,000 nodes, covering distances from 75 meters to several kilometers. The transmission rate ranges from 10 to 250 kb/s, with extremely low power consumption of only 1 mW. In addition, a ZigBee network can support 255 devices, with up to 100 networks in a region. It operates on flexible frequency bands, including 2.4 GHz, 868 MHz (Europe), and 902 MHz (USA), and offers various network configurations, such as star and mesh, supporting single-hop and multi-hop transmissions. Moreover, ZigBee ensures quick response times, high security with CRC and encryption algorithms, and high reliability through collision avoidance strategies and reserved time slots for conflict-free data transmission. Such technology relies on the IEEE 802.15.4 standard, maintained by the ZigBee Alliance, which has released several versions of the standard [15]. It provides a foundational security framework for ZigBee, including mechanisms for key establishment and device authentication. ZigBee leverages the security features of IEEE 802.15.4 to implement a secure network joining process, though challenges may arise in environments with a high density of devices [16]. As for data confidentiality and integrity, this protocol employs the AES-128 encryption algorithm to protect data transmission, ensuring a high level of data confidentiality and integrity. It also ensures data integrity and tamper resistance through Message Integrity Codes (MIC) or Message Authentication Codes (MAC). As for the resistance to replay attacks and signal interference, IEEE 802.15.4 utilizes Direct Sequence Spread Spectrum (DSSS) technology and multi-channel operation to reduce signal interference and enhance the reliability of data transmission.

2.4 WIFI

WiFi is a short-range wireless communication technology used to connect various devices including personal computers and mobile devices. Such network architecture includes

centralized and decentralized forms, with a coverage radius of up to 100 meters and data transfer speeds up to 600 Mb/s [5]. WiFi's evolution includes multiple standards, starting with IEEE 802.11 in 1997, operating in the 2.4 GHz band, and progressing to IEEE802.11a/b/g/n standards, covering the 5 GHz band and incorporating various modulation techniques and Multiple Input Multiple Output (MIMO) technology to enhance data transfer rates and network compatibility. The WiFi Alliance is responsible for establishing global standards, ensuring technological uniformity and device interoperability [9]. The protocol that will be discussed in this section is IEEE 802.11, which facilitates secure pairing through security protocols such as WPA and WPA2, and include a four-way handshake to authenticate and establish connections. Its upgrade version, IEEE 802.11i, has provide a enhanced security which introduced a stronger security architecture, including IEEE 802.1X for access control and AES encryption for data protection. The IEEE 802.11i standard ensures effective protection of data confidentiality and integrity by employing Counter-mode/CBC-MAC Protocol (CCMP), which utilizes the AES encryption algorithm. The protocol also offers TKIP (Temporal Key Integrity Protocol) as a transitional encryption method, though it is not as secure as CCMP [16]. As for the esistance to Replay Attacks and Signal Interference, IEEE 802.11 employs frequency hopping techniques to mitigate signal interference and incorporates sequence numbers and timestamps to resist replay attacks.

2.5 LoRa

LoRa, which refers to a low-power wide-area (LPWA) networking technology, facilitates long-range communication and is particularly beneficial for IoT applications that require minimal data payloads [6]. It has various of advantages, including extended battery longevity, substantial network capacity, and broad coverage. In comparison to alternative technologies, LoRa devices, along with their associated gateways and base stations, are cost-effective. Moreover, LoRa employs chip spread spectrum modulation techniques to achieve expansive coverage while conserving power. LoRa's open-hardware and open-source nature contribute to its ability to provide nationwide coverage with limited infrastructure. The LoRaWAN protocol employs symmetric encryption techniques and necessitates the secure exchange of keys during the pairing process. The backend interface of LoRaWAN facilitates the segregation of root key storage within the join server, ensuring that it acts as a trusted entity and thereby enhancing the security of the pairing process [16]. Additionally, LoRaWAN ensures data confidentiality and integrity by utilizing the AES-128 encryption algorithm. It supports end-to-end encryption, there for its difficult for intercepted data to be decrypted. Furthermore, both the MAC and application payloads in LoRaWAN are authenticated, integrity-protected, and encrypted, which safeguards the legitimacy of network traffic and the confidentiality of data. Designed with resistance to replay attacks, LoRaWAN employs unique random numbers,

such as DevNonce, for each network join request, ensuring its uniqueness and enhancing security. To combat signal interference, LoRaWAN uses Chirp Spread Spectrum (CSS) technology, which spreads the signal over a broad bandwidth, aiding in its distinction from background noise and improving resistance to interference.

3 Security Issues of Communication Protocols in IoT

3.1 EPC Gen2 in RFID

The EPC Gen2 protocol, while providing a secure pairing process through the use of an Access Password to restrict tag read/write operations, faces challenges due to the password's static and unchanging nature, as well as its plaintext transmission, which leaves it vulnerable to interception [10]. Additionally, its anti-collision mechanism may not perform efficiently in environments with multiple tags, indicating a need for further optimization. Although the protocol includes measures for data encryption and authentication, the security of RFID is often considered weak, especially in settings with limited resources, impeding the advancement of RFID technology. The static password, despite offering some protection against unauthorized data modification, does not effectively safeguard tag data due to its susceptibility to interception. Moreover, the protocol's design includes anti-collision features, but interference issues can still occur in areas with a high density of tags, suggesting that additional security enhancements are necessary. The static password also presents a risk for replay attacks, as intercepted passwords could be reused by attackers to carry out unauthorized actions [11].

3.2 IEEE 802.15.1 in Bluetooth

The IEEE 802.15.1 protocol, foundational to Bluetooth technology, has been instrumental in enabling short-range wireless communication. However, the protocol exhibits several limitations when evaluated against modern security and performance standards. Initially, the pairing process relied on static PIN codes, which are susceptible to brute-force attacks and compromising security [9]. The absence of advanced authentication mechanisms further exposed devices to potential man-in-the-middle attacks. Concerning data confidentiality and integrity, the encryption algorithms employed by the protocol are outdated and may not effectively counteract contemporary cryptanalytic techniques. The lack of a robust key management system also poses a risk, as it could lead to the extended use of identical keys, making them vulnerable to decryption. In terms of resistance to replay attacks, the protocol's use of timestamps and sequence numbers does not guarantee protection against all forms of such attacks. Additionally, Bluetooth devices operating under this protocol could experience signal interference from other wireless devices, especially in areas with high Wi-Fi network density.

3.3 IEEE 802.15.4 in ZigBee

The IEEE 802.15.4 protocol, while offering mechanisms for key establishment and device authentication, exhibits deficiencies, particularly in the security enhancements of the latest ZigBee versions, with notable flaws in the end-to-end application key establishment protocols [8]. In high-density device environments, identification and pairing processes may encounter challenges, leading to potential inefficiencies in secure pairing procedures. Despite the utilization of the AES-128 encryption algorithm, the IEEE 802.15.4 standard lacks specifications for key management and authentication strategies, leaving these critical issues to be addressed at higher layers by technologies such as ZigBee, which may result in suboptimal management of data confidentiality and integrity [16]. The constrained resources of ZigBee networks, including computational complexity and storage capacity, may impede the effective implementation of measures for data confidentiality and integrity. Furthermore, although Direct Sequence Spread Spectrum (DSSS) technology and multi-channel operation are employed to mitigate signal interference, ZigBee networks remain susceptible to interference from other devices operating in the 2.4 GHz band, particularly in signal-saturated environments. The multipath characteristics of wireless sensor network channels can adversely affect signal reception quality, leading to increased error rates, reduced battery life, and compromised network reliability.

3.4 IEEE 802.11 in WIFI

Despite the IEEE 802.11 protocol's provision for secure pairing through WPA and WPA2, vulnerabilities have been exposed in earlier versions such as WEP, revealing significant security flaws [5]. Even with the introduction of a more robust security architecture in the 802.11i standard, which includes 802.1X access control and AES encryption, practical challenges in secure pairing, such as device recognition and key management, persist. While protocols like CCMP and TKIP in the 802.11i standard aim to enhance data confidentiality and integrity, the security of these protocols hinges on the length of the keys and the robustness of the key management process. Data transmitted over radio waves is susceptible to interception by any Wi-Fi-enabled device in proximity, raising concerns of unauthorized access [17]. Furthermore, although IEEE 802.11 employs frequency hopping to mitigate signal interference, Wi-Fi networks remain vulnerable to interference from other devices operating in the 2.4 GHz band, including Bluetooth devices [18]. In terms of replay attacks, the use of sequence numbers and timestamps does enhance security. However, the possibility of disrupting information exchange sessions by sending deauthentication frames still poses a threat to security integrity.

3.5 LoRaWan in LoRa

The security of the pairing process in LoRaWAN protocols is potentially compromised due to their operation on the ISM free bandwidth and the public nature of their protocol specifications [6]. This may lead to diminished network security since attackers might intercept device addresses and dispatch malicious messages, or engage in "malicious crowding" attacks by occupying the channel with maximum length preambles. Although LoRaWAN employs the AES-128 encryption algorithm to safeguard data, its limited bandwidth results in low data transmission rates, typically ranging from several kilobits per second to tens of kilobits per second, which constrains its application in high bandwidth-requiring scenarios. While LoRaWAN's design accounts for resistance to replay attacks, its characteristics of low power and long-distance communication lead to significant transmission delays, typically ranging from several seconds to several minutes, rendering it unsuitable for applications demanding high realtime performance. Moreover, although LoRaWAN's utilization of spread spectrum technology to resist signal interference, it may still suffer interference in high-density network environments [19].

4 Possible Improvements

To enhance the security and performance of wireless communication protocols such as RFID, Wi-Fi, ZigBee, Bluetooth, and LoRa, several solutions can be implemented. These include deploying dynamic key management systems for regular key renewal, adopting robust encryption algorithms like AES-256 to strengthen data confidentiality and integrity, and ensuring end-to-end encryption of data during transmission to prevent leaks or tampering. The use of timestamps and sequence numbers in packets can verify the timeliness of data and prevent replay attacks. For protocols like Wi-Fi, additional security measures such as radio frequency fingerprinting can augment device pairing security, while adaptive frequency hopping techniques can help reduce signal interference in protocols like ZigBee [16]. Physical proximity in Bluetooth acts as a unique security feature, limiting unauthorized access through close-range communication. In RFID systems, particularly in high-density tag environments, optimizing anti-collision algorithms and enhancing access control to data areas are key to improving security. For LoRa, adaptive data rate algorithms can optimize communication parameters based on network conditions, and more advanced encryption standards can be explored to provide additional security layers. Power consumption can be reduced by optimizing transmission intervals and leveraging low-power features, ensuring longer battery life for IoT devices [6]. Careful planning of gateway placement and network topology can improve coverage and reduce the risk of signal interference, enhancing the reliability of LoRa networks.

These measures contribute to the overall security and performance of various wireless communication networks, ensuring secure and reliable data transmission.

5 Conclusion

As the performance and security of protocols keep advancing, it is anticipated that increasingly secure and efficient communication solutions will be developed to meet the growing demands for data transmission. The future of communication engineering may be centered on the development of intelligent systems capable of autonomously detecting and defending. These systems are expected to leverage artificial intelligence and machine learning algorithms to prevent potential attacks. In the realm of device pairing and data confidentiality, future communication protocols are likely to place a heightened focus on user privacy and data protection. By employing more robust encryption methods and secure pairing processes, communication engineering is poised to ensure that data transmission remains secure, even within open or untrusted networks. The capability to resist replay attacks and signal interference will also be a key consideration in future communication engineering. With improved protocol design and smarter channel management, communication systems will be equipped to overcome these threats, ensuring the reliability and integrity of data transmission. In conclusion, communication engineering will play an important role in the future of IoT. These technologies will not only facilitate efficient data transmission but will also guarantee the security and privacy of information. This will lay a solid foundation for the extensive application of IoT, ranging from smart homes to industrial automation, and onward to smart cities.

References

1. Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6:1606–1616, 04 2019.
2. Han J Y. Application analysis of communication engineering technology in internet of things. Audio Engineering, 46:130–132, 04 2022.
3. Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, and Siobhan Clarke. Middleware for internet of things: A survey. IEEE Internet of Things Journal, 3:70–95, 02 2016.
4. Iqbal H. Sarker, Asif Irshad Khan, Yoosef B. Abushark, and Fawaz Alsolami. Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 28:296–312, 03 2022.
5. Hui Dong, Jingran Tang, and Dongxing Yu. Development status and trend of iot communication technology. Communications Technology, 47:1233–1239, 11 2014.
6. Rocksan Choi, SeungGwan Lee, and Sungwon Lee. Reliability improvement of lora with arq and relay node. Symmetry, 12:552, 04 2020.

7. Zhang Yuqing Zhou Wei and Peng Anni. Survey of internet of things security. Journal of Computer Research and Development, 54:1–14, 06 2017.
8. Yang Y Y, Zhou W, Zhao S R, Liu C, Zhang Y H, Wang H, Wang W J, and Zhang Y Q. Survey of iot security research: threats, detection and defense. Journal on Communications, 42:188–205, 08 2021.
9. Santiago Figueroa Lorenzo, Javier An˜orga Benito, Pablo Garc´ıa Cardarelli, Jon Alberdi Garaia, and Saioa Arrizabalaga Juaristi. A comprehensive review of rfid and bluetooth security: Practical analysis. Technologies, 7:15, 01 2019.
10. Zilong Liu, Dongsheng Liu, Lun Li, Hui Lin, and Zhenqiang Yong. Implementation of a new rfid authentication protocol for epc gen2 standard. IEEE Sensors Journal, 15:1003–1011, 02 2015.
11. Wiem Tounsi, Nora Cuppens-Boulahia, Joaquin Garcia-Alfaro, Yannick Chevalier, and Fr´ed´eric Cuppens. Kedgen2: A key establishment and derivation protocol for epc gen2 rfid systems. Journal of network and computer applications, 39:152–166, 03 2014.
12. WEI He. Bluetooth technology development and its application prospection the internet of things. Applied energy technology, 4:52–54, 04 2016.
13. Ankur Jain and B K. Roy. Design and implementation of an iot ready smart sensor for speed sensing of a dc motor using ieee 802.15.1 and esp8266. International Journal of Engineering Technology, 7:974, 07 2018.
14. Deeksha Verma, Khuram Shehzad, Danial Khan, Qurat Ul Ain, Sung Jin Kim, Dongsoo Lee, Younggun Pu, Minjae Lee, Keum Cheol Hwang, Youngoo Yang, and Kang-Yoon Lee. A design of 8 fj/conversion-step 10-bit 8ms/s low power asynchronous sar adc for ieee 802.15.1 iot sensor based applications. IEEE Access, 8:85869–85879, 2020.
15. Dushyant Kumar Singh and Rajeev Sobti. Wireless communication technologies for internet of things and precision agriculture: A review. 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 6, 10 2021.
16. TAO Yufan LI Xiangyang ZHANG Weikang, ZENG Fanping. A survey for security of iot wireless protocols. Journal of Cyber Security, 7, 3 2022.
17. Xavier Silvani, Khaldoun Al Agha, Steven Martin, Daphn´e Goirand, and Nicolas Bult´e. Ieee 802.11 wireless sensor network for hazard monitoring and mitigation. Natural Hazards, 114:3545– 3574, 08 2022.
18. Seungku Kim. Bsense: Practical cross-technology communication utilizing beacon frames of commodity wifi aps. IEEE Transactions on Wireless Communications, 19:901–914, 02 2020.
19. Mohamed Eldefrawy, Ismail Butun, Nuno Pereira, and Mikael Gidlund. Formal security analysis of lorawan. Computer Networks, 148:328–339, 01 2019.