Journal of Cyber Security
DOI: 10.32604/jcs.2022.030498
Article

Tech Science Press

Analysis of Security Aspects in LoRaWAN

Ahmed AL-Hthlool[1,*] and Mounir Frikha[2]

[1]Ahmed AL-Hthlool, King Faisal University, Alhasa, 13890, Saudi Arabia
[2]Mounir Frikha, King Faisal University, Alhasa, 13890, Saudi Arabia
*Corresponding Author: Ahmed AL-Hthlool. Email: 221445321@student.kfu.edu.sa
Received: 26 April 2022; Accepted: 01 June 2022

Abstract: Nowadays, emerging trends in the field of technology related to big data, cognitive computing, and the Internet of Things (IoT) have become closely related to people's lives. One of the hottest areas these days is transforming traditional cities into smart cities, using the concept of IoT depending on several types of modern technologies to develop and manage cities in order to improve and facilitate the quality of life. The Internet of Things networks consist of a huge number of interconnected devices and sensors that process and transmit data. Such Activities require efficient energy to be performed at the highest quality and range, hence the concept of Long-Range Wide Area Network (LoRaWAN) introduced, which concerns about delivering lower energy consumption, supporting large networks and mobility. In this paper, the security mechanisms in LoRaWAN will be evaluated by literature review from many authors. The expected outcomes are to study and evaluate the LoRaWAN mechanism and class and protocol stacks.

Keywords: LoRaWAN; LoRa; cybersecurity; IoT

1 Introduction

The technology industry is evolving every day and it is impressive and scary at the same time, internet applications, internet of things (IoT) and computers are examples of technology and many others. IoT is a major technology by which can produce various useful internet applications. IoT can be defined as a network in which all physical objects are connected to the internet through network devices or routers and exchange data. IoT deal with a lot of devices and domains, and this can produce security issues for users that uses this technology like privacy, availability, confidentiality, and integrity as known CIA model.

As technology changing fast, developers must ensure users security of their data, especially when it comes to privacy, it is what people's concern about nowadays [1]. Security and privacy are the most important things in internet of things. Incorrect device update, absence of efficient and strong security protocols, lack of knowledge, and well-known device tracking are within the challenges that IoT is facing [2]. To make the users feal safe of their devices, the IoT security must be powerful. And to keep the security powerful the project interduces the concept of LoRaWAN and it is one of IoT applications.

LoRaWAN is low power wide area network protocol designed to connect to operated things to the internet in global, regional networks and targets internet of things. The distance required to receive and transmit data in LoRaWAN can be surrounded by 0.3 and 50 kbps [3]. The network architecture is deployed in as a star topology in which there are gateways and end devices, and they rely on each other and in between them central network server. The gateways are connected to network server via IP connections and act as a transparent bridge [3]. Example of LoRaWAN where it can be used in smart cities, homes, smart industry, and supply chain logistics. On the other hand, LoRaWAN suffers from some security problems like reply attack, bit flipping attack, eavesdropping and many others [4]. To keep security standers high is very difficult and challenging and it cannot be achieved straightforward. The purpose of this paper is to evaluate the security mechanism in the LoRaWAN. This includes a review and comparison of the current LoRaWAN protocol stacks, advantages and disadvantages of different security mechanisms applied in LoRaWAN. The security requirements introduced in LoRaWAN will be identified, and protocol stacks in LoRaWAN based on privacy, confidentiality, integrity, and availability will be compared. Rest of the paper is organized as section two is related work which is research of many authors in the felid of LoRaWAN, third section is LoRaSim which is the simulation tool for LoRaWAN, fourth section is recommendation which is the recommended papers for this research and lastly is the conclusion.

2 Related Work

Smart cities have developed as information and communication technologies as well as IoT is combined in cities to make the life of the people easier by upgrading operations and services [3]. Smart cities provide maintainable and cozy life with current resources by utilizing of theses now technology. It bargains services such as monitoring resources, enhancing current resources, and improving living conditions. All of those services are applied in many fields such as energy, traffic, education, environment, and security, and 70 percent of these services are focused in three parts: energy, security, traffic [4]. So, interaction between cultured structure and normal cities are now possible through IoT technology.

Smart technology contains applications that are physical, and they are capable to automatically adjust and alter behavior to fit an environment and feel objects with technology sensors. Smart technologies make contributes very crucial role in monetary development at city level. We can use this technology everywhere such as restaurants, offices, houses, hospitals, and all the cities can be changed into automatic and self-controlled systems acting on behalf of the human and thus broadcasting information to all of the people for news or any decision making can be done [5].

In this paper [6] the authors says that there are many challenges, such as spoofing and jamming attacks and accessing to file that is not authorized to access, which can compromise the integrity of the information. There are some possible solutions that can help any person to do many security precautions that will help to secure the IoT devices of the users. There are many privacy threats appeared in current days, and they can attack IoT devices and the network that is integrated with technology [7]. It is difficult handle the security of IoT devices in companies. The companies must monitor and have scanning tools for all the devices in IoT that might identify any threats associated with privacy and seek to reduce any risks are being violated.

Kumar Gupta [8] Review the concept of IoT and different deployed IoT devices from security perspective, including vulnerabilities, cyber-attacks, and countermeasures. The great development of technology and the exponential increase in the number of devices used to deploy the Internet of things raise the security and privacy concerns, especially with limited efforts served by manufactures and

service providers. Possible solution to overcome the security challenges is to develop a new protocol concern about data security. First, building a built-in system to counter automated attacks will mitigate the load and concentrate on other attacks. Other solution is based on observations, a plan is proposed to enhance the security system of IoT include the following: implementing firewall, firmware updating, implementing monitoring system, periodic passwords updating and raising the awareness for the users.

Miller [9] gives a brief overview of LoRaWAN and how LoRa and transmit and receive low amounts of data over wide range without expensive cost. Miller explained how to configure security protocol in LoRaWAN. He also explained the important things for LoRaWAN setup, and how the flow of process could jeopardize backend. He also presented a survey on the issues of LoRaWAN and to avoid the attacks or issues is by application that has a good key management practice. One of weaknesses of key management is the uses of symmetric encryption, where there are two places for the key to be stored, the nods and network server. Miller indicated that great solutions need to be developed to prevent any attacks for end users. By knowing cyber security of evert stage for the company, you can develop a different way to give LoRa solutions that fits the company needs.

This paper [10] talks about the burstiness of LoRaWAN network, and it has three classes A, B, C reflected to end user devices and to wide scope of users. This paper focuses of class A which is the default class for all end devices. End devices transmit data to gateways, and gateways delivers it to application server. Paper introduced a wildly protocol used called slotted ALOHA, which is a shared channel divided into discrete interval called time slot. The paper study's the impact of different burst length in the network performance, and the results shows when burst length increases the performance improves.

Chiang Rai [11] analyzes the LoRaWAN in terms of CIA modal and talk about the most important parameter that may harm this modal. Jhon McCumber invented a security cube that shows three aspects of security. First aspect is the CIA triad: confidentiality, integrity, and availability. The second aspect is data states, which is data operations, data at rest or in storage. And in last aspect is countermeasures, which is used to illustrate the disciplines, people, and skills to provide protection. The paper examined the vulnerability of the modal and shows the availability aspects of CIA modal is most affected, and the power of transmission increases the efficiency of contact.

Authors in [12] proposed a two-factor authentication based on blockchain for LoRaWAN. Blockchain is a system of recording information in a way that makes it difficult or impossible to change and it's a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. The author's objective is to propose two-factor of authentication primely based on blockchain for LoRaWAN to add extra layer of security in authentication system to construct trust with LoRaWAN end devices and servers. Authors simulated this framework using Ethereum blockchain and python client and the end devices for LoRa and network server. LoRaWAN network working in parallel with blockchain as an independent network and this framework has three stages. Setting up blockchain network is the first one which is deploying smart contract to network, which is a script that make blockchain more secure. After the reply from the address of smart contract, the device information is read from blockchain network and sends the transaction to gateway of smart contract. Initial authentication and registration are the second stage which validate the join request message by LoRaWAN network. Then the block id will be sent to network server, and it will be accepted by LoRaWAN end devices. Two-factor authentication is the third stage which is checking the receiving of the message of join request from network server and give block id saved from blockchain network server. If they match the network server will give the join accept message and end devices will

be connected. The result shows that the system provides great performance in condition of throughput and latency.

Authors in [13] is explaining how LoRaWAN enabling technologies under the area of smart cities and in order to gather data and process it, authors are evaluating and testing new methods and tools of different simulations to get the right or accurate results of LoRaWAN network. One of the examples of LoRa is non-culler merged with LoRaWAN medium access control (MAC) protocol used in LoRa system. It can be almost impossible to emulate a real-world scenario on a large network. In order to demonstrate the new contributions, they need to be evaluated. There are several network simulations and one of them is LoRaSim. The result shows that the authors analyze the nature of different LoRaSim implementations, and the different is having four groups of end devices and the parameters are payload, code rate, bandwidth and spreading factor. By applying a common propagation modal which is Okumura-Hata on the network that uses orthogonality between all devices, this diverseness increases its quality and efficiency.

In this paper [14] the authors propose a method to improve LoRa performance called sequencing transmission scheme. They used LoRaSim simulator to show the efficiency of the scheme. Authors said there will be an increasing number of sensors and IoT devices by 2030 and all transmission media will be crowed. LoRaWAN also no difference, the transmitted packet can be disrupted by collision or signal interference causing loss of packet and powdery of performance. So, to improve LoRaWAN performance authors propose sequencing transmission scheme which is non acknowledgement and non-repeating transmission. The end result showed that the scheme ought to offer as much as 100% data extraction rate (DER) while the assigned time become enough for every node to transmit and give 5%–10% average increase in DER compared to the normal LoRaWAN scheme.

Alexandru-loan and his associated authors [15] is focusing on LoRaWAN technology specially in LoRaSim simulator to explain bidirectional communication using LoRaWAN MAC protocol. Also, offer some insight into LoRaWAN overall performance based on network via many simulations. Low power wide area (LPWA) technologies offer to connect enormous numbers of devices that are distributed at low cost. With a log battery life and rage and keeping the cost down, LPWA is the alternative future of large-scale deployments. LPWA can transmit downlink, and that is important due it is required key for many applications in IoT, there are lots of network management function of LoRaWAN like network joining, handshaking etc. cannot be executed without the downlink key. So, to get the best network performance employing communication requires feedback from gateways to end devices and to inform that end devices should adopt their radio parameters, the gateways must keep an eye on the uplink signal quality. Results of this study shows LoRaWAN is affected negatively not only by the size of network, but also by attempts at retransmission and downlink traffic and it helps in reliability and throughput. Also, the paper emphasizes the careful selection of size of the network and parameter of LoRaWAN can give acceptable performance.

Authors in [16] discussing how to enhance and analyze duty cycle of LoRaWAN and how to protect it from attacks that could happened to it such as spoofing and bit flipping. ETSI regulations require each node to have maximum of 1% of duty cycle per cycle. This restriction can exclude critical applications that exceed the transmit messages per cycle channel authorized activity time. Authors also studied the vulnerability of dynamic in duty cycle and how it's influence by bit flipping and spoofing attacks to enhance LoRaWAN duty cycle. Bit flipping attack can be explained as changing a certain filed in cipher text without decryption, on the other hand spoofing attack is malicious attack used by hackers to pretend to be someone else and benefit from services freely. They proposed two solutions,

one is using the AppKey to protect LoRaWAN information to encrypt join request, other was mixing location of the bytes in the message and add hash function to get a secret key using AES OCB model.

Some modifications have been implemented in LoRaSim targeted to improve the ability of the tool to predict the performance of scalability of LoRa networks. These modifications give more accurate modeling of the propagation losses be more realistically modeled, also enable stable communications and configuration of network that is used for different propagation scenarios [17]. To improve the accuracy in predicting the number of sustainable nodes, authors did implement two main methods. They use three gateways and improve path loss evolution according to data extraction rate (DER). DER is the key used to evaluate the scalability of network and "it is defined as the ratio of received messages to transmitted messages over a period of time" [17]. The modifications made are to introduce the ability to test various models through different parameters and filed measurements of LoRa Received Signal Strength Indicator values.

Authors in this paper [18] focuses on handing LoRaWAN in physical layer that provide long distance and low power via Chirp Spread Spectrum (CSS) modulation. Open source on MAC protocol, community availability and support and the low-cost application are technologies of LoRa over other LPWAN. Authors proposed effective and simple method to enhance quality of service in LoRaWAN by adjusting certain radio parameters. Through problem formulation called mixed integer linear programming (MILP), they found out ideal settings for carrier frequency (CF) and spreading factor (SF) parameters considering the overall network traffic to enhance data extraction rate (DER) to reduce energy consumption and packet collision in LoRaWAN. They used LoRaSim for simulation result and it shows increasing in DER by 6% and a 13 times smaller number of collisions.

This paper discusses systematic review of LoRaWAN security protocol by finding vulnerabilities and what measurements can be taken for enhancement [19]. LoRaWAN protocol is an IoT application and it's part of large, interconnected devices, because of that it presents multiple vulnerabilities to attack whose aim is to access service or the data by modifying or blocking and damaging businesses and organizations that do not have adequate security mechanism in sight. Their methodology [19] of conducting systematic review was by the guidelines drawn up by Kitchenham. There are three phases which are planning, conducting, and reporting. In planning phase, asking the question that the systematic review is necessary or there is another equivalent research that gives expected results. In conducting phase, the study is continuing according to planning phase. In the first step, the investigation is carried out with the help of the search term and parameters. Then an evaluation is carried out to determine which study can help in answering the questions and met the specified criteria. Finally, an in-depth analysis of each study is performed to extract the data. In the report, when the data is extracted and compiled, it creates relevant information that can be used to answer the questions. Results show that 31 studies answered the primary questions and all of them helped in detecting vulnerabilities. 58.1% of them checked or tested for security vulnerability and 71% made for improvement.

Most popular assumption of LoRaWAN is uniformity of distribution timing of transmission of uplink packet through various machines that make up the network [20]. Recent studies have shown that this situation does not apply on real networks that consist of several devices and are operated with restriction on duty cycle. This study [20] turns to identifying the causes of this effect, which can potentially have a negative impact on the performance of the entire network. The paper also describing in detail the key aspect of LoRaWAN hypothesis, mechanism, and procedures that distribution of non-uniform of UL transmissions perhaps caused by effect of the over the air activation (OTAA). They

validate their hypothesis using simulations with specially developed model, which takes the subsequent data transmissions and information detail about OTAA in LoRaWAN.

LoRaWAN uses an energy efficient adaptive data rate (ADR) to allocate resources to end devices and that is recommended for static applications. Semtech [21] proposed using a blind ADR (BADR) to increase battery life for mobile application and geographic coverage. The purpose of this study is to analyze and give insight into the limits and potential of BADR. Simulation results show that regular ADR is not great for mobile application. On the other hand, BADR is great in energy consumption.

The article discussed the use of LoRaWAN wireless sensor nodes in smart IoT applications [22]. Their main idea is to reduce the power consumption of LoRaWAN wireless sensor nodes. They did an analysis of many components of energy consumption of architecture of wireless sensor nodes. In our everyday life, makes replacing or recharging batteries monetarily wasteful and time consuming. It's for those reasons and many others what drive the authors and researchers to find other source of energy to reduce the consumption of wireless sensor nodes. Results of the analysis shows that a precise identification of main energy consumption and analyze can lead to improve and apply energy effectiveness in wireless sensor nodes. Three scenarios have been made to show how they reduce the energy consumption. One of them is the new LoRaWAN energy efficiency protocol has reduced the battery power up to 30% and increase self-determining operation.

In this paper [23] authors talk about different technologies for battery and influence of physical and media access control layer (MAC) are examined. The readings examined in this senior includes impact on battery life and energy efficiency. Jarvis algorithm "its run on the sensor network to examine the impact on the MAC and physical layer of LoRa". Using this algorithm, they simulated using CupCarbon software the battery life, considering two of them, one nickel and other is lithium. The results show the stamina of lithium in state of charge is better than nickel and in voltage capacity. This can help in modeling sensor network and better energy efficiency. However, it has been observed that discharging of nickel battery over time using Jarvis algorithm different in days over lithium.

This study [24] is developing a proof of concept that includes the integration of open-source software and hardware components, and to detriment the operational coverage they developed an experimental methodology for LoRa network. This study provides a thorough understanding of properties and limitations of LoRa communications for real world applications with terron conditions, including driveways or obstacles can affect the performance of the network. Results shows that increasing spreading factor can increase coverage specially when it comes with industrial coverage environment.

Several connected devices and sensors are increasing every day, it is even more than the number of people having connection to global network [25]. Smart city has become mature and develop changes over last decade. But the service of smart city is becoming more popular in the global. Applications of smart city service are potentially covering many sectors such as consumption and disruption or energy production. All the new services require lots of control devices and monitoring sensors to connect between each other to manage the platform. Therefore, there is a need for new wireless communication network that can met the requirements of Smart City Services. LoRaWAN is a field of study for gateway coverage under different conditions show the attenuation coefficient under the city center and suburbs. The results shows that the signal was lost after 1500 m in the city and in the suburbs 1050 m maximum.

There is a new architecture for smart city which offer security and counter cyber-attacks. The proposed system [26] provides deep model based on machine learning to detect attackers depending on data behavior of the users. The variety of data structures, applications and the huge amount of

connections between devices in smart cities showed the necessity of using narrowband technologies. The main issue of these technologies is the restrictions that limit the security functionalities. Results have shown that the proposed methodology based on deep machine learning proved its efficiency in term of eliciting manner and data of attackers. The methodology can differentiate between normal users and attackers.

Authors of this article [27] uses a realistic network simulation to get insight into the actual performance LoRaWAN, and how even anything can affect the MAC layer even if it was small adjustments to the system performance. Authors highlight some inherent issues arising from duty cycle and suggested to do some improvement to mitigate the damage LoRaWAN may have on, such as device scale or network crowded. Results shows that in the standard configuration the presence of source acknowledgement traffic can significantly degrade the performance of unacknowledged traffic because of the additional interference created by downlink transmission. The critical factor seems to be signal gateway duty cycle restriction, which control the downlink channel and soon become the system's bottleneck when there were bidirectional streams.

Class A of LoRaWAN is designed to and focuses on the uplink and can have more battery life, on the other hand, class B an optional MAC operation is defined which gives the network server the ability to send downlink. The standard classes of LoRaWAN are not compared with the Class B performance. Authors of this paper [28] are proposing a rating for class B performance. They did a range of realistic assessments scenarios based on an NS3 simulation module developed by the authors. Authors is also doing study in depth for class B for transmission efficiency and delay for downlink comparing it with class A. the result showed that there is an improvement in class B performance in terms of access delay and data transfer efficiency compared to class A.

Authors in this paper [29] talks about review and discuss about Smart Lighting System and supported protocols used in IoT communications, which can be used to facilitate the Smart Lighting System. The lighting system is one of the main systems that have received great attention in IoT, which have proven that they can be developed greatly in addition to saving the energy wasted in this system. It was proved that lighting systems consumes a lot of energy comparing to other elements, which can be solved by IoT systems. The results showed that smart lighting systems reduced energy consumption by 33% for both outdoor and indoor sets.

Adaptive data rate (ADR) in LoRaWAN provides an interesting mechanism for self-depending on its settings to operating conditions. Many works have been developing and extending ADR for different use cases [30]. The authors in this paper give a review of ADR improvements with the aim of addressing the use cases of node mobility. The result confirmed that ADR improvement allow them to get high packet reception with node mobility.

This paper [31] propose to the usage of LoRa mobile gateway for smart electricity meters. LoRa transmission can be shortened with LoRa mobile gateway, the nearby system can use the same power of LoRa end device with less interference. Authors did the simulation using LoRaSim tool and did many scenarios with mobile gateway. LoRa uses unlicensed frequency below 1 GHz, and in the age of smart things this spectrum is overcrowded. Results shows that LoRa can be generally match the mobile gateway performance, and sometimes the performance can't be match due to lots of collisions. The energy consumption increases when number of nodes is increased. Also gets smaller when increasing time speed.

3 Recommendation

After this literature review search, we can say that most of the paper did not discuss about improving the security of LoRaWAN or finding the vulnerabilities. For example, in this paper did not discuss about the security side of LoRaWAN and in this paper [28] did not find more vulnerabilities that help this research. In our research these papers [20,23,24] could help us identify vulnerabilities and enhance security and duty cycle of LoRaWAN.

4 Conclusion

This survey paper introduced research in terms of security, vulnerabilities, and attacks of LoRaWAN and the different mechanism discussed by different papers from many authors. Papers from [3] to [8] also [25] and [26] is discussing the idea of the IoT and smart cities and how they are combined and important to make the life of the people easier by the services and operation they provide. While there are good side for IoT, there are some bad side for it which are the attacks. Most known attacks are spoofing and jamming. Rest of the papers are discussing how LoRaWAN is working, what are the class, what are the most attacks happened to it, how is it connected with IoT and smart cities, and how ADR and duty cycle are working. And there is a tool which can simulate attack happen in physical layer which is LoRaSim. What we recommend is following the papers who discussed more about the security of LoRaWAN and how it help to enhance it and what are the vulnerabilities and how to countermeasure it.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Georgios, 2017, "Security mechanisms for Internet of Things (IoT)," in *London: University of East London. J. Clerk Maxwell, A Treatise on Electricity and Magnetism*, 3rd ed., Oxford: Clarendon, vol. 2, pp. 68–73, 1892.

[2] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IOT privacy and security: Challenges and solutions," *Applied Sciences*, In: K. Elissa(Ed.), "Title of paper if known," unpublished. vol. 10, no. 12, pp. 4102, 2020.

[3] H. Noura, T. Hatoum, O. Salman, J. -P. Yaacoub, and A. Chehab, "Lorawan security survey: Issues, threats and possible mitigation techniques," *Internet of Things*, vol. 12, pp. 100303, 2020.

[4] J. C. Lee, J. H. Kim, and J. T. Seo, "Cyber attack scenarios on smart city and their ripple effects," in *2019 Int. Conf. on Platform Technology and Service (PlatCon)*, Korea, 2019.

[5] M. R. Belgaum, Z. Alansari, R. Jain, and J. Alshaer, "A framework for evaluation of cyber security challenges in smart cities," in *Smart Cities Symp. 2018*, America, 2018.

[6] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer IOT in the smart home: Architecture, challenges, and countermeasures," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 53–59, 2018.

[7] R. Chow, "Detecting privacy threats in IoT neighborhoods," in *Proc. of the 3rd ACM Int. Workshop on IOT Privacy, Trust, and Security*, ACM, 2017, Abu Dhabi, United Arab Emirates, pp. 23–30.

[8] S. K. Gupta, S. Vanjale, S. Rasal, and M. Vanjale, "Securing IOT devices in smart city environments," in *2020 Int. Conf. on Emerging Smart Computing and Informatics (ESCI)*, America, 2020.

[9] R. Miller. MWR Labs Whitepaper, "LoRa security building a secure LoRa solution," Available at: https://labs.f-secure.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf, [Accessed: 12-Oct-2021].

[10] A. Tsakmakis, A. Valkanis, G. A. Beletsioti, P. Nicopolitidis, and G. Papadimitriou, "On the effect of traffic burstiness in lorawan networks' performance," in *2020 Int. Conf. on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, Sharjah, United Arab Emirates, 2020.
[11] C. Kamyod, "CIA analysis for lorawan communication model," in *2021 Joint Int. Conf. on Digital Arts, Media and Technology with ECTI Northern Section Conf. on Electrical, Electronics, Computer and Telecommunication Engineering*, America, 2021.
[12] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi and M. Rajarajan, "A lightweight blockchain based Two factor authentication mechanism for LoRaWAN join procedure," in *2019 IEEE Int. Conf. on Communications Workshops (ICC Workshops)*, Shanghai, China, pp. 1–6, 2019. http://doi.org/10.1109/ICCW.2019.8756673.
[13] S. Francisco, P. Pinho and M. Luís, "Improving LoRa network simulator for a more realistic approach on LoRaWAN," in *2021 Telecoms Conf. (ConfTELE)*, Leiria, Portugal, pp. 1–6, 2021. http://doi.org/10.1109/ConfTELE50222.2021.9435570.
[14] K. Wongwatthanaroek and R. Silapunt, "Transmission sequencing to improve LoRaWAN performance," in *2021 18th Int. Joint Conf. on Computer Science and Software Engineering (JCSSE)*, Lampang, Thailand, pp. 1–5, 2021. http://doi.org/10.1109/JCSSE53117.2021.9493820.
[15] A. Pop, U. Raza, P. Kulkarni and M. Sooriyabandara, "Does bidirectional traffic Do more harm than good in LoRaWAN based LPWA networks?," in *GLOBECOM 2017–2017 IEEE Global Communications Conf.*, Singapore, pp. 1–6, 2017. http://doi.org/10.1109/GLOCOM.2017.8254509.
[16] N. Benkahla, B. Belgacem and M. Frikha, "Security analysis in enhanced lorawan duty cycle," in *2018 Seventh Int. Conf. on Communications and Networking (ComNet)*, Hammamet, Tunisia, 2018.
[17] S. Spinsante, L. Gioacchini and L. Scalise, "A novel experimental-based tool for the design of LoRa networks," in *2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT)*, Naples, Italy, pp. 317–322, 2019. http://doi.org/10.1109/METROI4.2019.8792833.
[18] E. Sallum, N. Pereira, M. Alves and M. Santos, "Performance optimization on LoRa networks through assigning radio parameters," in *2020 IEEE Int. Conf. on Industrial Technology (ICIT)*, Buenos Aires, Argentina, pp. 304–309, 2020. http://doi.org/10.1109/ICIT45562.2020.9067310.
[19] P. O. L. I. A. N. A. De moraes and A. R. L. I. N. D. O. Da conceição, "A systematic review of security in the LoRaWAN network protocol," 2021.
[20] K. Mikhaylov, "On the uplink traffic distribution in time for duty-cycle constrained LoRaWAN networks," in *2021 13th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Brno, Czech Republic, pp. 16–21, 2021. http://doi.org/10.1109/ICUMT54235.2021.9631708.
[21] A. Farhad, D. -H. Kim, J. -S. Yoon and J. -Y. Pyun, "Feasibility study of the LoRaWAN blind adaptive data rate," in *2021 Twelfth Int. Conf. on Ubiquitous and Future Networks (ICUFN)*, Jeju Island, Korea, pp. 67–69, 2021. http://doi.org/10.1109/ICUFN49451.2021.9528716.
[22] S. Asenov and D. Tokmakov, "Enhancing energy efficiency of LoRaWAN protocol," in *2021 12th National Conf. with Int. Participation (ELECTRONICA)*, Sofia, Bulgaria, pp. 1–5, 2021. http://doi.org/10.1109/ELECTRONICA52725.2021.9513667.
[23] E. Bermudez and D. F. H. Sadok, "Energy consumption of a LoRaWAN network using jarvis algorithm," in *2020 15th Int. Conf. for Internet Technology and Secured Transactions (ICITST)*, London, United Kingdom, pp. 1–6, 2020. http://doi.org/10.23919/ICITST51030.2020.9351345.
[24] C. Paternina, R. Arnedo, J. A. Dominguez-Jimenez and J. Campillo, "LoRAWAN network coverage testing design using open-source Low-cost hardware," *2020 IEEE ANDESCON*, vol. 1, pp. 1–6, 2020. http://doi.org/10.1109/ANDESCON50619.2020.9272128.
[25] A. V. Terleev, A. A. Khalturin and V. A. Shpenst, "LoRaWAN gateway coverage evaluation for smart city applications," in *2021 3rd Int. Youth Conf. on Radio Electronics, Electrical and Power Engineering (REEPE)*, Moscow, Russia, pp. 1–4, 2021. http://doi.org/10.1109/REEPE51337.2021.9388004.
[26] I. E. Asmaa Elsaeidy, *A Smart City Cyber Security Platform for*, Australia: IEEE, pp. 978–1–5090–6796–1, 2017.

[27] D. Magrin, M. Capuzzo and A. Zanella, "A thorough study of LoRaWAN performance under different parameter settings,"*IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 116–127, 2020, http://doi.org/10.1109/JIOT.2019.2946487.

[28] H. E. Elbsir, M. Kassab, S. Bhiri and M. H. Bedoui, "Evaluation of LoRaWAN class B efficiency for downlink traffic," in *2020 16th Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Thessaloniki, Greece, pp. 105–110, 2020. http://doi.org/10.1109/WiMob50308.2020.9253405.

[29] A. A. Amit Kumar Sikder, *IoT-enabled Smart Lighting Systems for Smart Cities*, Padua: IEEE, pp. 978–1–5386–4649–6, 2018.

[30] N. Benkahla, H. Tounsi, Y. -Q. Song, and M. Frikha, "Review and experimental evaluation of ADR enhancements for Lorawan networks," *Telecommunication Systems*, vol. 77, no. 1, pp. 1–22, 2021.

[31] S. Sugianto, A. A. Anhar, R. Harwahyu and R. F. Sari, "Simulation of mobile LoRa gateway for smart electricity meter," in *2018 5th Int. Conf. on Electrical Engineering, Computer Science and Informatics (EECSI)*, Malang, Indonesia, pp. 292–297, 2018. http://doi.org/10.1109/EECSI.2018.8752818.