An Open Source LoRaWAN Simulator Framework for the Internet of Things Applications

Sahel Alouneh
Cybersecurity program
Al Ain University
Abu Dhabi, UAE
sahel.alouneh@aau.ac.ae
Computer Eng. Dept.
German Jordanian University
sahel.alouneh@gju.edu.jo

Ala' Khalifeh
Electrical Eng. Dept.
German Jordanian University
Amman, Jordan
ala.khalifeh@gju.edu.jo

Dhiah el Diehn I. Abou-Tair
Computer Science Dept.
German Jordanian University
Amman, Jordan
dhiah.Aboutair@gju.edu.jo

Khaled Aldahdouh
Computer Eng. Dept.
German Jordanian University
Amman, Jordan
khaledaddahdouh@hotmail.com

Feras Al-Hawari
Computer Eng. Dept
German Jordanian University
firas.alhawari@gju.edu.jo

***Abstract*—LoRaWAN which stands for the Long Range Wide Area Network is an emerging wireless technology that is expected to be widely deployed and used, especially with the promising widespread use of the Internet of Things (IoT) applications and the Fifth Generation (5G) communication technology. In this paper, we proposed an enhancements framework for the widely used LoRaSim open source simulator. The proposed enhancements will enable the user to fine-tuning various parameters on LoRaWAN simulated networks according to application requirements, investigate and analyze the security effects on LoRaWAN IoT communication links, and adding more functionality pertaining the nodes' energy consumption.**

Keywords—security, LoRaWAN networks, IoT, simulator, Fifth Generation 5G

I. Introduction

In recent years, remote sensing and monitoring systems gained huge momentum from several sectors worldwide, due to the importance of monitoring large areas with minimal cost and effort. Moreover, the technological advances in the semiconductor industry led to finding more suitable solutions for wireless and remote monitoring applications by developing lower costs and higher efficiency modules that can be used for these applications [1]. Fifth Generations (5G) networks are considered as the key enabler for future Internet of Things (IoT), where more than 50 billion devices are expected to be connected to the global IP network [2], the predictions about connected IoT devices show that the connection density will rise to 10^6 devices/ km^2 [3].

Several key enabling technologies have been proposed recently as promising candidates for the Fifth-Generation and beyond networks, targeting diverse requirements for remote sensing and monitoring of applications, which require long communication range, low energy consumption, and low bandwidth. Such systems can be implemented using Low Power Wide Area (LPWA) networks, such as LoRaWAN, SigFox, and Narrow Band IoT (NB-IoT), which are the technologies in use for deploying the networks that require long-range transmission [4].

- *Why LoRaWAN networks?*

LoRa is a physical layer technology developed by LoRa Alliance in 2015 and used to address the requirements of long-range transmission and low data rates networks. It cancels the need for repeaters between the sensor nodes and the gateway (base station), so it reduces the nodes' cost and increases the battery life of nodes [5]. It uses the Industrial, Scientific, and Medical (ISM) frequency band which is an unlicensed radio spectrum (EU: 868MHz and 433MHz, USA: 915MHz and 433MHz) [5]. To obtain low power specifications and increase the communication range, LoRa uses Chirp-Spread Spectrum (CSS) modulation, which has been used in long-range transmission and military applications because of its ability to overcome interference and the losses in the long-distance transmission. Therefore, an entire city can be covered under only one gateway, so it is suitable and compatible with IoT network requirements [6]. LoRa is the radio modulation technology for wireless LAN networks while LoRaWAN defines the global communication protocol and the system architecture for LoRa networks [7]. LoRa enabled sensor node consists of three parts; a sensor to sense the environment, a microprocessor to process the sensed data, and a radio module with an antenna to transmit and receive the data. LoRa gateway, which can listen to multiple frequencies at the same time, consists of two parts; microprocessor and radio module [7].

Figure 1 depicts an overall view of LoRaWAN network for IoT applications and transmissions. LoRa device can be configured using five transmission parameters that determine the communication specifications, and the five parameters are:

1. Transmission Power: (TP) refers to the power of the transmitted signal of LoRa entities. Transmitted power is

in the range from – 4 to 20 dBm. However, due to hardware limitations, this range changes to 2 to 14 dBm. The signal can be decoded at the receiver when its power is ≥ the sensitivity SRX value [8, 9].

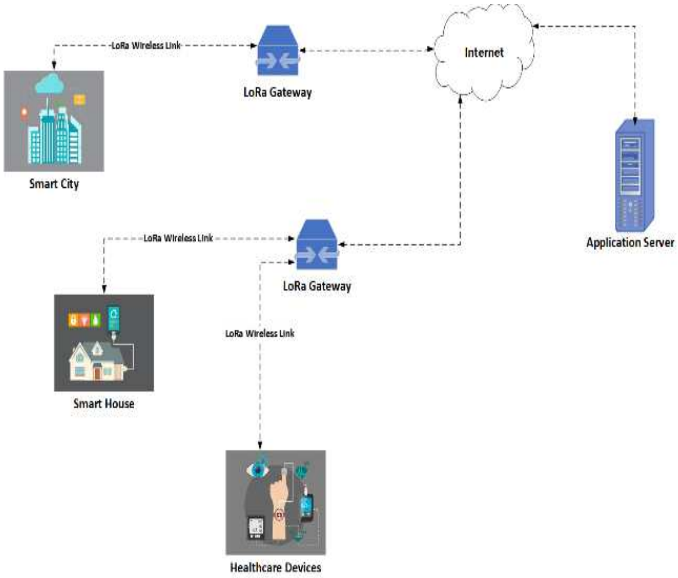


Fig. 1. LoRa network for IoT applications: Examples of LoRaWAN smart applications: smart cities, healthcare devices, and smart houses.

2. Bandwidth: (BW) value is the width of transmitted signals frequencies. BW can be configured to be in the range of 7.8KHz to 500 KHz, with a step of power of 2 (i.e., BW_2= 2×BW_1). Common values of BW are 125, 250, and 500 KHz [2, 3]. Higher BW value leads to higher data transmission rates, increased spread out, and less delay (i.e., *time on air*). Nevertheless, higher data rate leads to more noise interference and lower reception sensitivity.

3. Carrier Frequency: (CF) is the center frequency of a transmitted signal. It can be configured in the range from 137 to 1020 MHz where the step frequency value is 61 Hz [8, 9].

4. Spreading Factor: (SF) is the number of bits encoded in each symbol. It can be configured to be in the range from 6 to 12. The number of chips per symbol is represented by 2 SF. For example, SF = 6 means 2^6 = 64 chips per symbol is used. High SF values lead to higher sensitivity and increased communication distance. However, this will lead to lower data transmission rates, higher latency (time on-air delay), and higher power consumption. If SF is increased by 1, this will double the power consumption, and the air on time latency, and the sensitivity will increase by 3dB.

5. Coding Rate: (CR) represents the Forward Error Correction (FEC) rate that is used to protect against data interference. CR configuration values can be set to be: 4/5, 4/6, 4/7, or 4/8. Higher CR values lead to higher protection but also lead to higher data size so higher latency (time on-air).

Another important factor for having a reliable LoRa based communication is security. Therefore, the consideration of LoRa's security is an important and ongoing research problem. In reference [15], the risk analysis of LoRaWAN networks is presented with future directions. Security in Low Powered Wide Area Networks, including LoRa networks, has been investigated in [16] with a focus on opportunities for Software-Defined Network-Supported solutions. The authors in [17] discussed the design of a Blockchain-Based IoT using three technologies: Ethereum, Swarm, and LoRa. The research focuses on providing software solutions to create high availability with minimal security risks. A novel modeling key generation approach for LoRa networks is presented in [18]. In [19], a case study is presented for IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. A useful recent survey on LoRa Networking is presented in [20 , 21] with a focus on Research problems, current solutions, and open issues including considerations for security issues.

II. Proposed Work

A. Aims and Objectives

There are several attempts by researchers targeting to provide an enhanced open-source LoRa simulator that can be used by researchers to study and simulate LoRa based networks. Nevertheless, the simulators in use have shortcomings which will be discussed in detail in the research methodology section.

To evaluate the network performance, a LoRa simulator is often used to collect some initial results according to different cases in which different numbers of LoRa nodes are placed with different sink nodes in the 2-D space.

A "smart node" in the network has its parameters: Transmission Power, Spreading Factor, Carrier Frequency, Bandwidth, and Coding Rate. In addition, each smart node transmission behavior is described by the average packet rate (ʎ) and packet payload (B), so each node is described by (TP, CF, SF, BW, CR, B, ʎ).

Two metrics are used to evaluate the performance of LoRaWAN networks. These metrics are the Data Extraction Rate (DER) and Network Energy Consumption (NEC) that are defined below.

DER = received packets / transmitted packets in a specific duration (DER must be maximum).

NEC is the total energy consumption in LoRa transceiver nodes. (NEC must be minimum).

The expected findings should help in improving the performance of LoRaWAN networks by:

A- Reducing the congestion in network Gateways.

B- Reducing packet loss.

C- Reducing interference.

D- Improving the security

Therefore, the main objectives of this proposed work are summarized as follows:

- Provide the research community with an enhanced and open source LoRaWAN simulator that utilizes the reinforced machine-learning possible algorithms (e.g., deep reinforcement learning) to better optimize the selection of the LoRa various parameters and study its performance under different network conditions.
- It is worth mentioning that security applications to any communication system will have an impact on its performance, e.g., power consumption. Therefore, security considerations for LoRa networks is an important objective which will be studied and investigated in this work. The goal of this research is to come up with a generalized LoRa-Security framework that will pave the way towards possible implementations for LoRaWAN simulators.

Consequently, our ultimate objective is to study the feasibility of applying our enhanced LoRa simulator in real environment like Abu Dhabi IoT platforms (whether in public or private sectors) with security considerations in mind.

B. Research Methodology

Our enhanced LoRa simulator will be based on available open-source LoRa simulators. In the open literature, several researchers attempted to provide an Open Source simulator that can be used by researchers to study and simulate LoRa based networks. In particular, LoRaSim [11] was first proposed by researchers from Lancaster University, which was used in several publications such as [12, 13]. The LoRaSim simulates LoRa networks with the option of having several base stations, different number of nodes, and different radio settings of network nodes. However, LoRaSim has the following limitations:

- Accepts only a limited number of inputs of parameters (two values of the Spreading Factor, two values of bandwidth, two values of Code Rate, and three values of Central Frequency.
- All the nodes use single transmission power.
- The output of each simulation run is the Data Extraction Rate and the total power consumption in the network

To address these limitations, the authors in [14, 15] proposed a modified version of the LoRaSim where the following features have been added:

- The transmission parameters inputs are all the possible values of CF, SF, and PT values.
- The modified simulator has two types of nodes, a normal and smart node. The normal node is assigned fixed parameter values that do not change during the simulation duration. Whereas the smart node parameters can be changed during the simulation duration depending on the acknowledgment of the received packets. Consequently, the parameters value can be optimized during the simulation duration using a machine learning reinforced learning algorithm.
- This modified LoRa simulator uses a reinforcement-machine learning approach to select the optimal values of different entered parameter values, mainly: the SF, CF, and transmission power for a given network scenario. However, these values are modified for the smart nodes after each transmission, while the parameters of the normal nodes remain the same as the first transmission settings and do not change during the simulation time.
- The modified LoRaSim allows to have more input parameters to the simulation environment such as the total number of normal nodes n_1, the number of smart nodes n_2, where n_2 is less than or equal to n_1, the number of gateways, the average sent time, the total simulation time, the size of the simulation area, and the payload size.
- The modified LoRaSim allows a random distribution of the gateways in the simulation area of interest.
- The modified LoRaSim uses the well-known EXP3 reinforced learning algorithm [12] to determine the best values of SF, CF, and PT from input values of each node in the network. Then, it modifies these values for the smart nodes after each transmission.
- In the modified LoRaSim, all nodes have the same values of CR and BW.
- The output of the simulator is the received data packet rate and the total consumed power in the network.

III. Enhancements On The Modified LoraSim

The proposed enhancements in our simulator build up the following features on top of the work in [12, 13], where the following features will be considered in the proposed framework:

- Allowing the user to input all possible values of the BW, SF, and CR. In addition, the input value of PT is set to be the maximum available power value.
- All the nodes can be smart (no differentiation between normal and smart nodes).
- Allowing more optimized distribution of gateways (i.e., no random distribution).
- In addition to existing outputs of the modified LoRaSim, the enhanced simulator adds the per-node power consumption output. Therefore, it allows us to analyze the node's time in a network.
- Investigating the possibility of using other reinforcement-machine learning algorithms and not only the EXP3 algorithm.

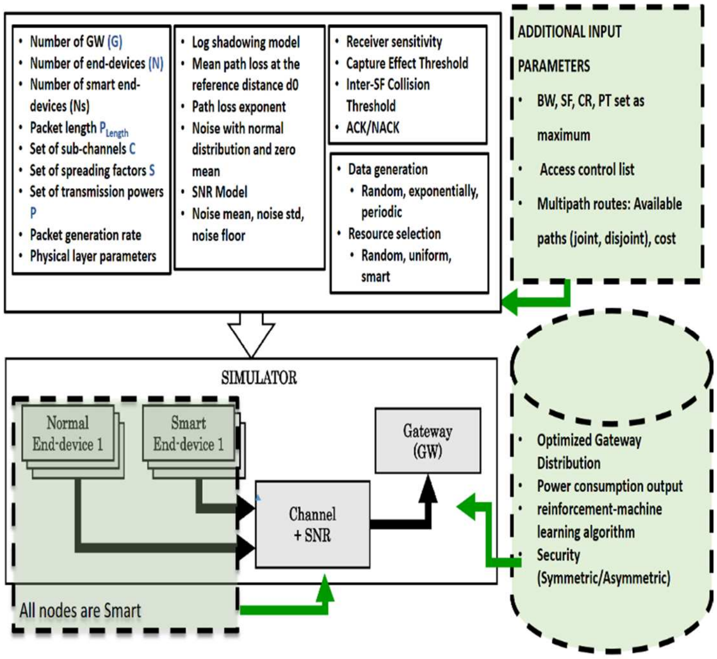
Our proposed simulator framework for LoRaWAN security relies on the adoption of multi-path routing to address the following security parameters. Figures 3 depicts the security and multipath enhancements as follows:

- Data communication confidentiality: confidentiality is needed to encrypt transmitted data while in communication, and therefore not being disclosed to unauthorized entities. We propose to enable LoRaWAN with multi-path capabilities so that transmitted signal should follow *k* path channels towards the receiving node. In this way, *k* Sub-Coded-transmitted signals (K_SC) are assigned to the *k* multipath channels. Each SC signal carries a codded signal where no useful information can be disclosed if it has been captured by an unauthorized entity. It is worth mentioning that using conventional encryption techniques such as AES, DES should consume more power compared to sending plain data signals. Therefore, sending SC coded signals in multipath should consume lower bandwidth and processing power [22]. The proposed simulator framework should consider LoRaWAN multipath and also single path channel transmission type. For example, cryptographic algorithms standard will be integrated within the LoRa simulator framework. Multiple key length sizes such as 128 and 256 bits will be considered for AES encryption techniques. This work will investigate the application feasibility of both key sizes. It is worth noting that a key length of 256 bits is practically unbreakable by brute force based on current computing power, making it the strongest encryption standard, however, we should investigate its impact on LoRaWAN network performance, especially the power consumption factor. Also, the simulator framework will also examine the impact of multipath routing and compare the results with AES technique.
- Integrity of data: this term "Integrity" refers to data communication integrity and reliability. In data integrity, the receiver can be sure that the received data has not been modified during its path channel. In this work, a framework for multipath LoRa-data-integrity will be proposed and simulated. We propose to enable LoRaWAN with multi-path capabilities so that transmitted signal should follow *k* path channels towards the receiving node. For data reliability, the proposed framework requires to add a redundant path channel(s) where the number of redundant channels is equal to: Redundancy *R*= *n*-*k*.

Overall View On The Simulator

In summary, Figure 2 below shows a diagram for the overall enhancements to be carried out by this work on LoRaWAN based simulators in [11-14]. The dashed blocks in the figure show our proposed enhancements.

The simulation process of the enhanced LoRaWAN simulator is presented in Figure 3. First, each end-device generates a packet using a random distribution procedure, like the exponential distribution. The packet generation speed is selected to fulfill the duty cycle limit. The generated packet after that is transferred to the gateway by choosing the selected radio resources. The security layer and multipath routing should be integrated between the end devices, channels, and the gateways.



Number of GW (G)
Number of end-devices (N)
Number of smart end-devices (Ns)
Packet length P_{Length}
Set of sub-channels C
Set of spreading factors S
Set of transmission powers P
Packet generation rate
Physical layer parameters
Log shadowing model
Mean path loss at the reference distance d0
Path loss exponent
Noise with normal distribution and zero mean
SNR Model
Noise mean, noise std, noise floor
Receiver sensitivity
Capture Effect Threshold
Inter-SF Collision Threshold
ACK/NACK
Data generation
Random, exponentially, periodic
Resource selection
Random, uniform, smart
ADDITIONAL INPUT PARAMETERS
BW, SF, CR, PT set as maximum
Access control list
Multipath routes: Available paths (joint, disjoint), cost
SIMULATOR
Normal End-device 1
Smart End-device 1
Gateway (GW)
Channel + SNR
All nodes are Smart
Optimized Gateway Distribution
Power consumption output
reinforcement-machine learning algorithm
Security (Symmetric/Asymmetric)

Fig. 2. The suggested diagram of the enhanced LoRaWAN simulator. Enhancements are marked using dashed lines

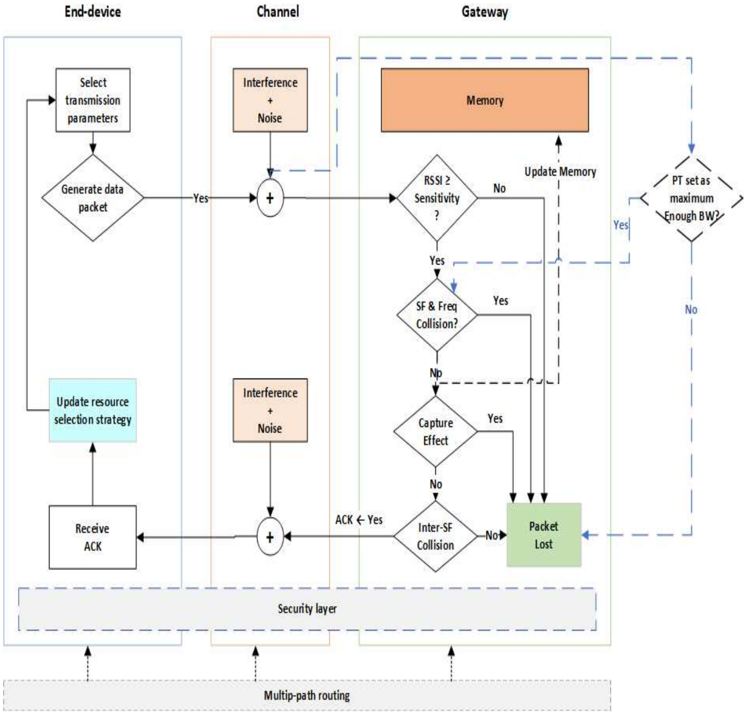


Fig. 3. The framework for the simulation process [13], the proposed enhancement is presened using dashed line.

IV. Conclusion

LoRaWAN has very wide-ranging applications. A list of applications consists of smart supply chain and logistics, smart cities, smart agriculture businesses and processing, smart buildings, smart gas metering, smart electricity metering, and smart healthcare. In order to effectively deploy this technology, several performance-determining parameters need to be optimized and fine-tuned, depending on the application under consideration. To achieve that, network simulation is a key solution environment that will enable researchers to investigate the effect of changing several LoRa parameters and enable them to investigate how these parameters affect the transmission performance and Quality of Service (QoS). The contribution of this work aims at providing the research community with a framework for an enhanced LoRaWAN simulation tool which builds upon existing simulators, namely LoRaSim [11]. The proposed enhancement is related to : 1) The power consumption, 2) The security considerations (i.e., confidentiality and data/user authentication) and 3) The integration of Reinforced machine-learning algorithms to optimize the selection of the LoRaWAN parameters. Our proposed enhanced simulator framework offers the following advantages over current simulation tools such as: enabling users to fine-tuning various parameters on LoRaWAN simulated networks according to application requirements, investigating and analyzing the security effects on LoRaWAN IoT communication links and adding the per-node power consumption output.

References

[1] Goudos, S. K., Dallas, P. I., Chatziefthymiou, S., & Kyriazakos, S. (2017). A survey of IoT key enabling and future technologies: 5G, mobile IoT, sematic web and applications. Wireless Personal Communications, 97(2), 1645-1675.

[2] Mitra, Rupendra Nath, and Dharma P. Agrawal. "5G mobile technology: A survey." ICT Express 1.3 (2015): 132-137.

[3] De Almeida, I. B., Mendes, L. L., Rodrigues, J. J., & da Cruz, M. A. (2019). 5G Waveforms for IoT Applications. IEEE Communications Surveys & Tutorials.

[4] Mekki, Kais, et al. "Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT." 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2018.

[5] Ala' Khalifeh; Khaled Aldahdouh; Sahel Alouneh, "Optimizing the Energy Consumption Level in LoRaWan Networks",21st International Arab Conference on Information Technology (ACIT), 2020.

[6] Sinha, Rashmi Sharan, Yiqiao Wei, and Seung-Hoon Hwang. "A survey on LPWA technology: LoRa and NB-IoT." Ict Express 3.1 (2017): 14-21.

[7] Zhou, Q., Zheng, K., Hou, L., Xing, J., & Xu, R. (2018). X-LoRa: An Open Source LPWA Network. arXiv preprint arXiv:1812.09012.

[8] Voigt, T., Bor, M., Roedig, U., & Alonso, J. (2016). Mitigating inter-network interference in LoRa networks. arXiv preprint arXiv:1611.00688.

[9] Bor, M. C., Roedig, U., Voigt, T., & Alonso, J. M. (2016, November). Do LoRa low-power wide-area networks scale. In Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (pp. 59-67). ACM

[10] https://www.lancaster.ac.uk/scc/sites/lora/lorasim.html

[11] Bor Martin C., Utz Roedig, Thiemo Voigt, and Juan M. Alonso. "Do LoRa low-power wide-area networks scale?." In Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pp. 59-67. 2016.

[12] Voigt, Thiemo, Martin Bor, Utz Roedig, and Juan Alonso. "Mitigating inter-network interference in LoRa networks." arXiv preprint arXiv:1611.00688 (2016).

[13] Ta, D. T., Khawam, K., Lahoud, S., Adjih, C., & Martin, S. (2019, September). Lora-mab: A flexible simulator for decentralized learning resource allocation in iot networks. In 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC) (pp. 55-62). IEEE.

[14] Ta, Duc-Tuyen, Kinda Khawam, Samer Lahoud, Cédric Adjih, and Steven Martin. "Lora-mab: A flexible simulator for decentralized learning resource allocation in iot networks." In 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), pp. 55-62. IEEE, 2019.

[15] Pathak, G.; Gutierrez, J.; Rehman, S.U, "Security in Low Powered Wide Area Networks: Opportunities for Software Defined Network-Supported Solutions", Electronics, 9, 1195. 2020.

[16] K. R. Ozyilmaz and A. Yurdakul, "Designing a Blockchain-Based IoT With Ethereum, Swarm, and LoRa: The Software Solution to Create High Availability With Minimal Security Risks," in IEEE Consumer Electronics Magazine, vol. 8, no. 2, pp. 28-34, March 2019, doi: 10.1109/MCE.2018.2880806.

[17] Gao, W. Xu, S. Kanhere, S. Jha and W. Hu, "Poster Abstract: A Novel Modeling Involved Security Approach for LoRa Key Generation," 2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Sydney, Australia, 2020, pp. 327-328

[18] I. Max, M. Jims, B. Deepayan, "IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN", IET Information Security, 14, (4), p. 368-379. 2020.

[19] D. Heeger and J. Plusquellic, "Analysis of IoT Authentication Over LoRa," 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, CA, USA, pp. 458-465. 2020.

[20] J. P. Shanmuga Sundaram, W. Du and Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues" in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 371-388, 2020.

[21] A. Khalifeh; K. Aldahdouh; K. A. Darabkh; W. Al-Sit, " A Survey of 5G Emerging Wireless Technologies Featuring LoRaWAN, Sigfox, NB-IoT and LTE-M", 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET).

[22] Alouneh, S., Abed, S., Kharbutli, M. et al. MPLS technology in wireless networks. Wireless Netw 20, 1037–1051 (2014).