LoRaWAN Energy Optimization with Security Consideration

Ala Khalifeh[1], Khaled Aldahdouh[1] and Sahel Alouneh[1,2]
[1]School of Electrical Engineering and Information Technology, German Jordanian University, Jordan
[2]College of Engineering, Al Ain University, UAE

Abstract: *Long Range Wide Area Network (LoRaWAN) is an emerging wireless technology that is expected to be widely deployed and implemented in several applications, especially with the promising widespread use of the Internet of Things (IoT) and its potential applications within the Fifth Generation (5G) communication technology. LoRaWAN consists of a number of nodes that monitors and senses the environment to collect specific data, and then sends the collected data to a remote monitoring device for further processing and decision-making. Energy consumption and security assurance are two vital factors needed to be optimized to ensure an efficient and reliable network operation and performance. To achieve that, each of LoRaWAN nodes can be configured by five transmission parameters, which are the spreading factor, carrier frequency, bandwidth, coding rate and transmission power. Choosing the best values of these parameters leads to enhancing the network deployment. In this paper, we shed the light to the security aspect in LoRaWAN network. Then, we introduced an algorithm that depends on the reinforcement learning approach to enable each node in the network to choose the best values of spreading factor and transmission power such that it leads to a lower energy consumption and higher packets' delivery rate. The results of the simulation experiments of our proposed technique showed a valuable increase in the packet reception rate at the gateway and a significant decrease in the total consumed energy at the end nodes compared with the most related work in literature.*

Keywords: *LoRaWAN, transmission parameters, reinforcement learning, power consumption, Security, Confidentiality, Authentication.*

Received February 28, 2021; accepted March 7, 2021
https://doi.org/10.34028/iajit/18/3A/11

1. Introduction

Nowadays, remote monitoring systems became a necessary requirement in many applications and systems, especially with IoT services. Furthermore, the revolution in semiconductors and microelectronics helped to design enhanced modules, which can be used to overcome the limitations of the current remote monitoring applications [8]. Fifth Generation (5G) is the revolution that supports the future of IoT applications, where more than 50 billion nodes will be connected to the internet [16]. It is expected that the future connected IoT density will exceed 10^6 nodes per km^2 [6]. Many wireless technologies have been examined to implement remote sensing and monitoring applications in the fifth generation of communication systems. Low Power Wide Area (LPWA) technologies like LoRaWAN, SigFox, and Narrow Band IoT (NB-IoT) are good technologies, which are tested to be used within the Fifth Generation system [15].

LoRa technology was introduced in 2015 to meet the requirements of long communication range with low data rate. LoRa technology eliminate the need to use repeaters between the end device and receiver, which in turn leads to decrease the cost of the communication links between the sensor nodes and the gateway, reduce the power consumptions, and increase the lifetime of the network [14]. LoRa technology utilizes the Industrial, Scientific, and Medical (ISM) frequency band that varies between the regions (e.g., EU: 868MHz and 433MHz, USA: 915MHz and 433MHz) [14].

LoRa protocol utilizes Chirp-Spread Spectrum (CSS) modulation scheme to obtain lower consumed energy and longer communication range compared to other technologies. This modulation supports the communication over long distances due to its ability to overcome the noise and interference level in the communication link. Therefore, it is commonly used in several military applications. These specifications make LoRa technology proper to implement IoT networks [21]. It must be mentioned that LoRa is the Local Area Network (LAN), while LoRaWAN is the global protocol that connects LoRa networks [26]. Each one of LoRa nodes must be configured using five different transmission parameters. The values of these parameters determine the specifications of the network, in terms of bandwidth, transmission range and speed. These parameters are:

- Transmission Power (TP): It is the power of the signal transmitted from the node, its value ranges from -4 dBm to 20 dBm in 1dBm step, but due to the hardware constraints, its range becomes from 2dBm

to 14 dBm. The gateway can receive the signal if the received power is higher than (or equal) the sensitivity of the gateway (S_r). The signal can be successfully decoded by the receiver if its power is 20dB less than the noise floor, thus it can meet the requirements of long communication range using extremely low transmission power [1, 24].

- Carrier Frequency (CF): it is the carrier frequency of the transmitted signal. Its value is according to the ISM band ranges from 137 MHz to 1020 MHz in 61Hz step [1, 24].
- Spreading Factor (SF): it is the ratio between the symbol rate and the chip rate. It has six values from 7 to 12 in a step of 1. SF=12 means 2^{12} chips/symbol. Using higher SF leads to better receiver sensitivity and higher transmission range, but this will also lead to less data rates and more delay (time on air). Different SF values are considered orthogonal, i.e. the gateway can decode two signals with the same center frequency if they have different SFs [1, 24].
- Bandwidth (BW): it is the range of the frequencies in the transmitted signal. Its values are from 7.8 KHz up to 500 KHz in a step of power of 2 ($BW_2 = 2BW_1$). The typical values are 125 KHz, 250 KHz, and 500 KHz [1, 24]. Higher BW means higher data rates, longer transmission range, and lower latency (time on air), but this will lead to more noise, more interference and less receiver sensitivity [1, 24].
- Coding Rate (CR): it is the amount of error detection and correction capability, which is utilized to increase the protection of the transmitted signal from the interference. Its values are 4/5, 4/6, 4/7, or 4/8. The 4/8 means that there are 4 extra bits for each 4 actual bits, while 4/5 means that there is only one extra bit for each 4 data bits. Two end nodes can communicate with each other even if they have different CR values. Higher CR leads to more protection, but also leads to longer message, so more time on air [1, 24].

The most challenge in LoRa networks is the energy optimization and conservation. The amount of the consumed energy is based on the transmission parameters values, thus it is important to choose the optimal values of these parameters to decrease the consumed power and increase the network lifetime. This work continues our previous works [5, 11, 12] that proposed techniques to optimize the consumed energy in Wireless Sensor Networks (WSNs). In this work, we developed technique to optimize the consumed energy in LoRa networks, which will be a useful candidate for WSN. The proposed work takes into account the link behaviour to enable each node to choose the optimal value of the spreading factor and transmission power parameters. The distance from the node to the gateway and the spreading factor value play an essential role in determining the transmission power parameters. The transmission power value can be adjusted automatically based on the network requirements and the link conditions, this leads to decreasing the energy consumption and improving the performance in LoRa networks. Furthermore, the paper proposes a security framework for LoRaWAN and how it may affect the energy consumption.

This paper is an extended version of our conference paper [13], where more details and simulation results are added. In addition, a security framework for LoRaWAN is proposed.

The next sections are organized as the following: the related work is presented in section 2, LoRaWAN security framework is presented in section 3. Section 4 presents the proposed technique to determine the optimal values of the spreading factor and transmission power parameters. Section 5 presents the simulation experiments and the results' discussion. Finally, the conclusion of the paper is listed in section 6.

2. Related Work

Many techniques have been introduced to decrease the power consumption level in LoRa networks. In what follows, the most relevant literature work to our proposed research are summarized.

Bor *et al*. [1] studied the capacity limitations and how Data Extraction Rate (DER) and Network Energy Consumption (NEC) are affected by increasing the density of LoRa network. The authors did some practical experiments to derive the behaviour model of the network. Then they developed a simulator called "LoRaSIM" that describes the scalability of LoRa networks. The practical experiments were repeated in several days by varying the number of nodes in the network (up to 1600) with different parameters values. The authors found that the DER decreased from 95% to less than 60%, and the NER increased from less than 200 mJ to more than 300 mJ when increasing the number of nodes from 100 to 600.

In another study, To and Duda [23] developed a technique to reduce the collision level at the gateway and total consumed energy in the network by using Carrier Sense Multiple Access (CSMA) protocol rather than ALOHA (Additive Links On-Line Hawaii Area) in LoRa nodes. The authors used NS-3 simulator to examine their proposed work. They built a network with different number of nodes (up to 10000 nodes) and reported the total consumed energy and the collision level. The simulation results were compared with practical measurements conducted by previous works. They noticed that at low number of nodes (less than 1500), the collision level reduced from 20% to 5%, but the total consumed energy increased slightly from 6000 mJ to 7000 mJ. At higher number of nodes (from 1500 to 4000), the variance in the consumed energy is less than 200 mJ and the packet reception rate is higher (from 60% without CSMA to 90% with CSMA). At larger number of nodes (higher than 4000), the author

found that the total consumed energy is significantly lower (from 12000 mJ without CSMA to 8000 mJ with CSMA), and the packet reception rate is higher (from 10% to 60%) which makes the total throughput of the network higher.

Bor and Roedig [3] studied the effect of different values of LoRa transmission parameters on the consumed energy and the packet reception rate. They developed a technique for selecting the transmission parameters values automatically according to the network requirements. Two nodes (sender and receiver) were used for different practical experiments using 1152 different combinations of the transmission parameters. The sender node is configured to transmit 255 packets of 32 bytes. The practical experiments were repeated several times for about 34 hours. The sender node transmitted about 1.6 million packets. The authors found that at the best configuration settings, 3.5% of the transmitted packets were lost, 6% were corrupted, and 90.5% were successfully received. The consumed energy was 2 mJ for each transmitted packet.

Ochoa *et al*. [18] studied the physical layer of LoRa technology and proposed many designs to modify LoRa parameters values in different scenarios to obtain more data rates or higher distance at lower consumed energy. The authors did simulation experiments in both star and mesh topologies using nodes that send packets of 50 bytes at different values of spreading factor, bandwidth and transmission power. Then the power consumption in the network is reported. EU frequency band was used to transmit the packets, and Okumura Hata propagation model was implemented. The consumed energy was considered during both sending and receiving the packets. According to the simulation results, the authors found that at a range less than 3 km, the minimum power consumption was met at TP = 2 dBm, BW = 500 KHz, and SF=6. For higher ranges, the bandwidth value must be adjusted based on the data rate. The authors suggested that in a star topology, the minimum energy consumption is obtained by adjusting the values of the transmission parameters. However, in mesh topology, the minimum consumed energy was obtained by changing many factors such as the hop count, density of the network and base station coverage.

In other work, Javanovic *et al*. [10] developed a model that measures the moisture of the soil remotely by a wireless module that utilises a high transmission power value to obtain long range up to 10 km. The authors accomplished a long distance range by consuming large transmission power value. They did not focus on how the system can be self-operational.

Ta *et al*. [22] utilized reinforcement learning approach to choose the best values of the transmission parameters for each end node in LoRa network. The authors proposed a technique to choose the best spreading factor, center frequency and transmission power values. Exponential weights for Exploration and Exploitation (EXP3) algorithm [22] was used, where the received acknowledgment is the primary factor that is used to adjust the parameters values. According to the proposed algorithm, the reward is 1 if the node received an acknowledge for the transmitted packet, otherwise the reward is 0. The weights of the transmission parameters are modified based on the reward value of each node. The authors developed a simulator to work according to their proposed algorithm. They called it LoRaWAN-ML [7], which is based on LoRaSim simulator [2]. The authors did some simulation experiments using circular area with radius of 4.5 km and measured the packet reception rate. The nodes send a packet of 50 bytes each 4 minutes. Bandwidth was set to 125 KHz and code rate 4/5 was used. The center frequency value is chosen from the values (868100 KHz, 868300 KHz, and 868500 KHz). The transmission power value is chosen from the values (8, 11, and 14 dBm), and the available spreading factor values are (7 to 12). The capture effect threshold is set to be 6 dB. EXP3 algorithm chooses the optimal values of SF, TP and CF based on their weights on each node. The convergence time of their proposed algorithm, the required time to determine the best parameters values for each node, was too long (about 200 Khours). At this time, the reception packet ratio was about 90%, and the average consumed energy for each transmitted packet was about 0.2 J.

LoRaWAN security was recently addressed in several research papers [4, 17, 25] In particular, Noura *et al*. [17] presented a survey on the most critical security and privacy threats to LoRaWAN. Furthermore, countermeasures and mitigation procedures against these threats were proposed and discussed. Yang *et al*. [25] discussed several LoRaWAN security features such as key management, message acknowledgement, activation methods, ciphering, and counter management. Furthermore, the authors examined several LoRaWAN vulnerabilities and attacks using a controlled environment such as replay attack, plaintext recovery, malicious message altering, delivery reports falsifications, and battery exhaustion attacks. Finally, Claverie and Lopes-Esteves [4] proposed a benchmark tests for LoRaWAN security assessment, which can be used to evaluate the network security and identifies vulnerabilities.

3. LoRaWAN Security Framework

In this section, we propose a preliminary security framework for LoRaWAN where several security considerations and enhancements are proposed for the LoRaWAN simulator used in this paper. In particular, the following factors are emphasized:

- Confidentiality of data: meaning the data is secure and encrypted so that it is not disclosed while in communication [19]. It is worth mentioning that encrypted data communication consumes more power than plain data. Therefore, a framework for

LoRa-Confidentiality data communication is paramount, where certain confidentiality algorithms and protocols should be used as seen fit for IoT environments. For example, cryptographic algorithms standard will be integrated within the enhanced LoRaWAN simulator. These standards will have multiple key length sizes (128 and 256 bits), where application feasibility of both key sizes should be studied. 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, the key-size impact on LoRaWAN network performance, especially the power consumption factor should be well studied. Furthermore, certain robustness considerations for post-quantum techniques if redeemed possible within these environments should be proposed.

- Integrity (Authentication): this term "Integrity" refers to two security features: data and user integrity. The integrity aspect involves data integrity and data origin validation or authentication.. The authentication means the identical setup to recognize the connected devices [9]. In data integrity, the receiver can assure that the data has not been modified. The data origin authentication verifies to the receiver that the stated source or sender has created the data. Therefore, having a framework for LoRa-data-and user authentication is an essential component to guarantee the network operation security and authenticity.
- Access-Control List (ACL) is another crucial component for the proposed security framework. This component can be named as LoRaWAN-ACL. ACLs are a network filter employed by routers and some switches to permit and limit data flows into and out of network interfaces. When an ACL is configured on an interface, the network device analyses data passing through the interface, compares it to the criteria described in the ACL, and either permits the data to flow or prohibits it. There are varieties of reasons we use ACLs. The primary reason is to provide a basic level of security for the network. Figure 1 shows our proposed Security Framework for LoRaWAN networks which works in parallel with energy utilization. First, each end-device generates a packet using a random distribution procedure, like the exponential distribution. The packet generation speed is selected to fulfil the duty cycle limits including security requirements. The main security aspects that are considered are:

a) Data Encryption using either Advanced Encryption Standard (AES) or Data Encryption Standard (DES) techniques.
b) Data Authentication using Message Digest Algorithm Five (MD5) or Secure Hash Algorithms (SHA) techniques.
c) User authentication using digital signatures.

Availability by using rigid ACL lists. The generated packet after that is transferred to the gateway by choosing the selected resources. The Gateway is responsible for evaluating the security requests sent by the end-device. If the security requests can be accommodated by the network with consideration to energy capabilities, then an Acknowledgement (ACK) is granted to allow a secure channel transmission. Otherwise, a Negative ACK (NAK) is initiated and sent to End-device.

4. LoRaWAN Nodes Transmission Parameters Optimization

In this section, an algorithm is developed that is based on the work presented in [22]. This algorithm enables each node to choose the best spreading factor and transmission power values such that it improves the transmission efficiency and energy consumption. The other transmission parameters, which are the coding rate, center frequency and bandwidth, are predetermined in the nodes. The proposed algorithm uses the EXP3 algorithm to find the best spreading factor values for the nodes. Then the receiver sensitivity can be determined based on the chosen spreading factor and the predetermined bandwidth according to Table 1.

Table 1. The sensitivity of the receiver at different SF, BW values.

SF	Receiver sensitivity [dBm] at BW=125KHz	Receiver sensitivity [dBm] at BW=250KHz	Receiver sensitivity [dBm] at BW=500KHz
7	-126.5	-124.25	-120.75
8	-127.25	-126.75	-124
9	-131.25	-128.25	-127.5
10	-132.75	-130.25	-128.75
11	-134.5	-132.75	-128.75
12	-133.25	-132.25	-132.25

The receiver sensitivity Sr can be expressed by Equation (1) [20]:

$$Sr = -174 + 10\log(BW) + NF + SNR \quad (1)$$

Where the value -174 is the thermal noise at BW=1Hz, which depends on the receiver temperature. NF is the receiver noise floor, which depends on the receiver hardware design. SNR is the required signal to noise ratio to decode the arrived signal at the gateway, which depends on the used SF value [1].

On the other side, the path loss value of the link from the node to the gateway depends on the well-known log-distance path loss model [1, 20] as in Equation (2):

$$Lp(d) = Lp(d0) + 10\,\gamma\log\left(\frac{d}{d0}\right) + X_6 \quad (2)$$

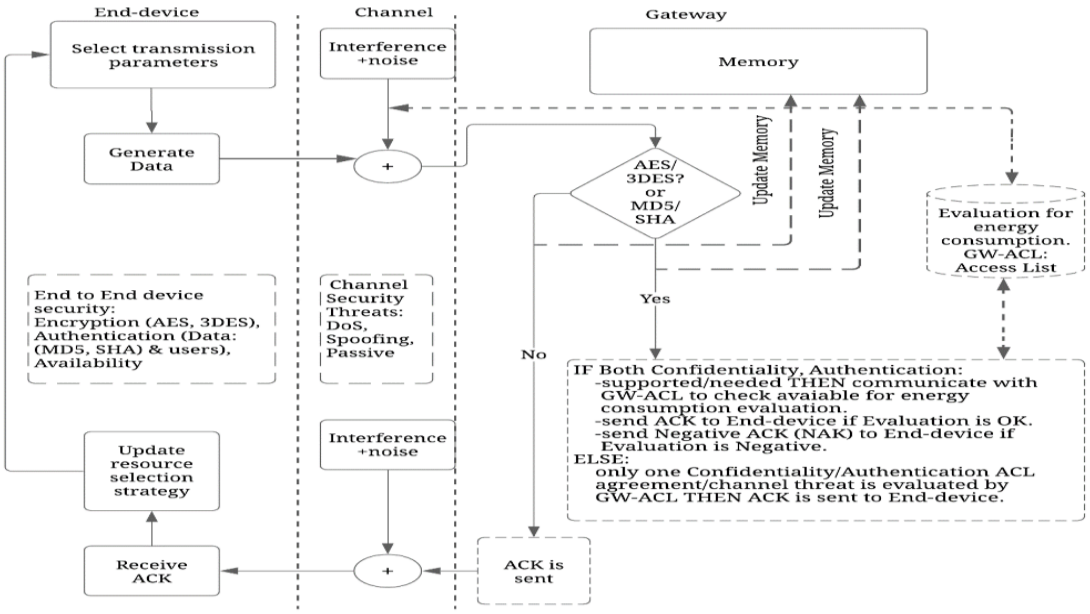

Figure 1. Security framework for LoRaWAN networks.

Where *Lp(d)* represents the path loss (in dB) for distance *d*, $Lp(d_0)$ represents the path loss value for referenced distance d_0, Υ is the path loss exponent value, and $X\sigma$ represents the normal of shadowing, it has zero mean and σ^2 variance, $X\sigma \sim N(0, \sigma^2)$ [1]. At distance $d_0 = 40m$, the measured path loss is 127.41dB, the path loss exponent Υ is 2.08, and the normal shadowing $X\sigma$ is 3.57 [1]. If the distance between the end node and the gateway is known, then the path loss of the link *Lp(d)* can be determined. In this work, we assume that each node has the location(s) of the gateway(s) and has a Ground Position System (GPS) receiver to identify its location, thus the distance between the node and the gateway can be calculated. Moreover, if the sensitivity of the receiver (*Sr*) is determined, the minimum required value of the Transmission Power (*PT*) for each node can be determined according to Equation (3):

$$PT = Sr + Lp(d) \quad (3)$$

Finally, the value of the transmission power parameter must be an integer number in the range from -2dBm to 20 dBm. Therefore, the ceil function is used to round up the result of TP of the node to the next integer number.

5. Simulation Results and Performance Analysis

We developed LoRaWAN-ML simulator, which was used in [22], to implement our proposed algorithm. To obtain the total consumed energy in the network; three simulation experiments were conducted at different available SF values to enable the EXP3 algorithm to choose the best one of them for each node. In the first experiment, two SF values are used (7 and 8). In the second experiment, four SF values are used (7, 8, 9, and 10), while all SF values are used (7, 8, 9, 10, 11, and 12) in the third experiment. Finally, some simulation experiments were performed to obtain the packet reception rate at the gateway, and then we compared our results with the ones presented in [22]. All the simulation experiments have the settings listed in Table 2.

Table 2. Simulation parameters.

Payload size	50 bytes
Simulation area	4 km*4 km
Number of nodes	100
Center frequency	868.100 MHz
Bandwidth	125 KHz
Coding rate	4/5
Packet generation rate of the node	15 packets per hours (1 packet per 4 minutes)
Simulation times	(20,40,60,80,100)*4 minutes
Maximum Transmission power	14 dBm

In what follows, the simulation results in terms of nodes' total power consumed and packets' reception rate are presented and discussed.

5.1. The Network Total Power Consumption

In the following, the simulation results of our proposed algorithm are shown and compared with the proposed work in [22] at the same settings. We must mention that in [22], the authors used three values of the transmission power parameters as input for the EXP3 algorithm (8, 11, and 14 dBm), whereas our proposed algorithm determines the minimum required transmission power value for each node. Therefore, our proposed algorithm is expected to spend less energy and improve the network performance compared to the work proposed in [22]. We used different simulation times for each simulation experiment.

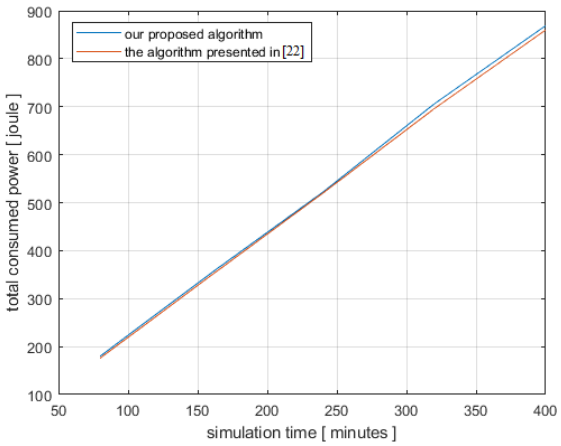

Figure 2. The total consumed energy using SF 7 and 8.

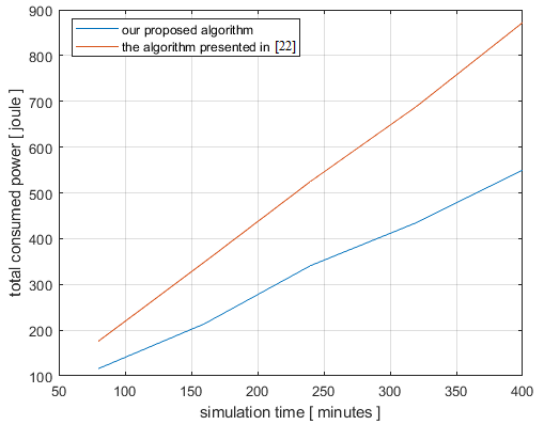

Figure 3. The total consumed energy using four SF values: 7, 8, 9, and 10.

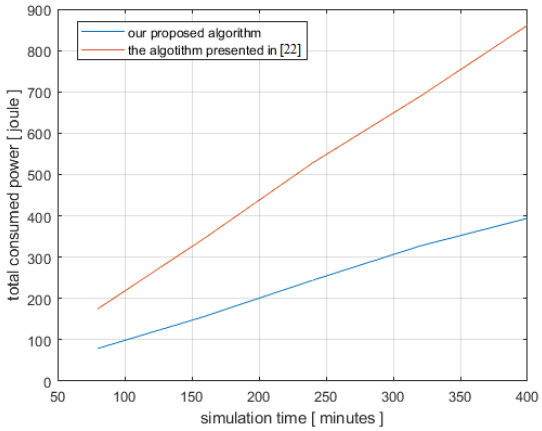

Figure 4. The total consumed power using all SF values.

Figure 2 shows that the consumed power using SF7 and SF8, which is almost the same, and it increases from about 95 joules at simulation time of 80 minutes, to about 870 joules at simulation time of 400 minutes. Figures 3 and 4 prove that the total consumed power using our proposed algorithm is clearly lower compared to the algorithm in [22]. This is because that the nodes in our algorithm use the minimum required transmission power value, but the nodes in the algorithm presented in [22] use one of only three available values for the transmission power. Figure 3 shows the total consumed power using SF values 7, 8, 9, and 10. The consumed power in our proposed algorithm increased from about 55 joules at simulation time 80minutes to about 550 joules at simulation time of 400minutes. However, the total consumed power according to the algorithm in [22] increased from about 90 joules at simulation time of 80minutes to about 870 joules at simulation time of 400minutes. Figure 4 shows the simulation results for the total consumed power using all SF values. The consumed power in our proposed algorithm increased from about 40 joules at simulation time of 80minutes to about 400 joules at simulation time of 400minutes. However, according to the algorithm in [22], this value increased from about 90 joules at simulation time of 80minutes to about 860 joules at simulation time of 400minutes.

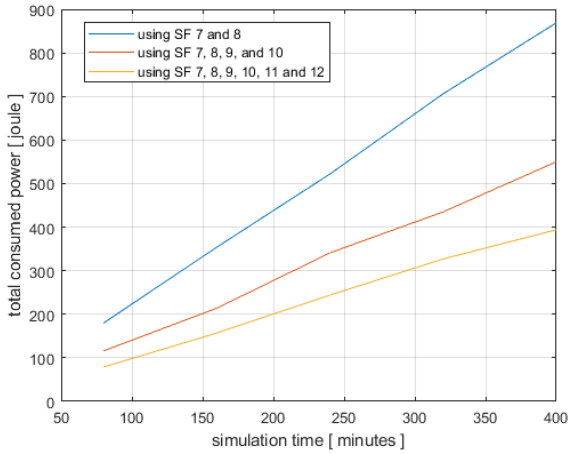

Figure 5. The total consumed energy in the new algorithm at different SF values.

Figure 5 shows the total consumed power according to our technique at different SF values, it is clear that the total consumed power decreases when there are more available SF values. This is because at higher SF value, the node supports higher communication range and better receiver sensitivity (less received power is required). Thus, the required transmission power of the node is lower.

5.2. The Total Packet Reception Rate at the Gateway

The packets' reception rate depends on the collision level between the arrived packets at the gateway. When two or more packets arrive the gateway at the same time with the same transmission parameters, the gateway cannot decode them due to the collision between the two packets. Therefore, it is necessary to enable the nodes that transmit at the same time to select at least different SF values. This will reduce the collision as possible, thus increase the packets' reception rate at the gateway.

Figure 6 shows a comparison between the packets' reception rate at the gateway at different number of nodes in the network using our proposed algorithm and using the algorithm presented in [22].

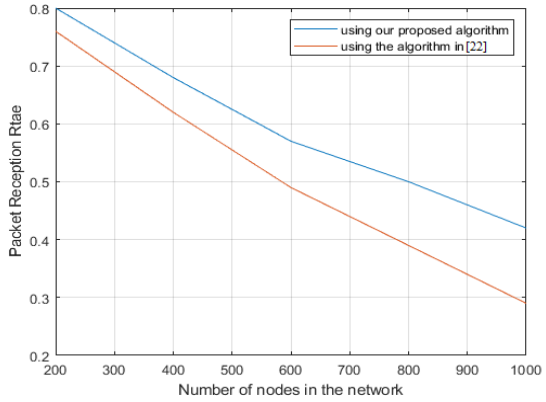

Figure 6. The packets' reception rate at the gateway.

It is clear from Figure 6 that the packets' reception rate using our proposed algorithm is higher than the algorithm proposed in [22], which means that the collision levels using our proposed algorithm is lower compared to the algorithm in [22]. This is because the nodes, according to our proposed algorithm, use different values of transmission power, which is determined according to the node's transmission parameters and location with reference to the gateway. However, in [22], the nodes use one out of three values of the transmission power, which lead to increasing the collision level between the arrived packets at the gateway.

6. Conclusions

In this paper, we presented an algorithm that chooses the optimal value of the spreading factor and the minimum required value of the transmission power for each node in the network based on the sensitivity of the receiver and the path loss of the link between the node and gateway. Our work utilizes the reinforcement learning to choose the best values of spreading factor, center frequency and transmission power. Furthermore, we proposed a security framework for LoRaWAN that can be adopted to ensure the network security and availability. Our simulation results were compared with the results of other similar techniques presented in related work in term of the total consumed power in the network and the packet reception rate at the gateway. The comparison showed a clear increase in the packet reception rate and a significant decrease in the consumed power when we used all the values of spreading factor.

Acknowledgment

The work presented in this paper has been supported in part by the German Jordanian University, under the seed grant No. SEEIT 02/2018.

References

[1] Bor M., Roedig U., Voigt T., and Alonso J., "Do LoRa Low-Power Wide-Area Networks Scale," *in Proceedings of the 19th International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Malta, pp. 59-67, 2016.

[2] Bor M., "LoRaSim Simulator Based on SimPy for Simulating Collisions in LoRa Networks and to Analyses Calability," https://www.lancaster.ac.uk/scc/sites/lora/lorasim.html, Last Visited, 2021.

[3] Bor M. and Roedig U., "LoRa Transmission Parameter Selection," *in Proceedings of the 13th International Conference on Distributed Computing in Sensor Systems*, pp. 27-34, 2017.

[4] Claverie T. and Lopes-Esteves J., "A LoRaWAN Security Assessment Testbench," *in Proceeding of the GNU Radio Conference*, vol. 2, no. 1, 2021.

[5] Darabkh K., Kassab W., and Khalifeh A., "Lim-AHP-G-C: Life Time Maximizing Based on Analytical Hierarchal Process and Genetic Clustering Protocol for the Internet of Things Environment," *Computer Networks*, 176, 2020.

[6] De Almeida I, Mendes L., Rodrigues J., and Cruz M., "5G Waveforms for IoT Applications," *IEEE Communications Surveys and Tutorials*, vol. 2, no. 3, pp. 2554-2567, 2019.

[7] Duc-Tuyen Ta., "LoRaWAN-ML Network Simulator with Reinforcement Learning-Based Algorithms," https://gitlab.com/tuyen.ta/lorawan-ml, Last Visited, 2021.

[8] Goudos S., Dallas P., Chatziefthymiou S., and Kyriazakos S., "A Survey of IoT Key Enabling and Future Technologies: 5G, Mobile IoT, Sematic Web and Applications," *Wireless Personal Communications*, vol. 97, no. 2, pp. 1645-1675, 2017.

[9] Houhamdi, Z. and Athamena B., "Identity Identification and Management in the Internet of Things," *The International Arab Journal of Information Technology*, vol. 17, no. 4A, pp. 645-654, 2020.

[10] Jovanovic U., Jovanovic I., Petrusic Z., and Mancic D., "Low-Cost Wireless Soil Moisture Monitoring System," *Facta Universitatis, Series: Working and Living Environmental Protection*, aol. 11, no. 2, pp. 87-95, 2015.

[11] Khalifeh A., Abid H., and Darabkh K., "Improving Energy Conservation Level in WSNs by Modifying CH Node Location," *in Proceedings of the Accepted for Publication at the 6th International Workshop on Internet of Things: Networking Applications and Technologies*, Paris, pp. 20-23, 2020.

[12] Khalifeh A., Abid H., and Darabkh K., "Optimal Cluster Head Positioning Algorithm for Wireless Sensor Networks," *Sensors*, vol. 20, no. 13, 1-26, 2020.

[13] Khalifeh A., Aldahdouh K., and Alouneh S., "Optimizing the Energy Consumption Level in

LoRaWan Networks," *in Proceedings of 21st International Arab Conference on Information Technology* , 6th of October city, pp. 1-6, 2020.

[14] Khutsoane O., Isong B., and Abu-Mahfouz A., "IoT Devices and Applications Based on Lora/Lorawan," *in Proceedings of The 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, pp. 6107-6112, 2017.

[15] Mekki K., Bajic E., Chaxel F., and Meyer F., "Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT," *in Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops*, Athens, pp. 197-202, 2018.

[16] Mitra R. and Agrawal D., "5G Mobile Technology: A Survey," *ICT Express*, vol. 1, no. 3, pp. 132-137, 2015.

[17] Noura H., Hatoum T., Salman O., Yaacoub J, and Chehab A., "LoRaWAN Security Survey: Issues, Threats and Possible Mitigation Techniques," *Internet of Things*, vol. 12, 2020.

[18] Ochoa M., Guizar A., Maman M., and Duda A., "Evaluating LoRa Energy Efficiency for Adaptive Networks: From Star to Mesh Topologies," *in Proceedings of the 13th International Conference on Wireless and Mobile Computing, Networking and Communications*, Rome, pp. 1-8, 2017.

[19] Palaniswami S. and Rajaram A., "An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad Hoc Networks," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 291-298, 2012.

[20] Petajajarvi J., Mikhaylov K., Roivainen A., Hanninen T., and Pettissalo M., "On the Coverage of LPWAN: Range Evaluation and Channel Attenuation Model for LoRa Technology," *in the Proceedings of 14th International Conference on ITS Telecommunications*, Copenhagen, pp. 55-59, 2015.

[21] Sinha R., Wei Y., and Hwang S., "A Survey on LPWA Technology: LoRa and NB-IoT" *ICT Express*, vol. 3, no. 1, pp. 14-21, 2017.

[22] Ta D., Khawam K., Lahoud S., Adjih C., and Martin S., "LoRa-MAB: A Flexible Simulator for Decentralized Learning Resource Allocation in IoT Networks," *in Proceedings of 12th IFIP Wireless and Mobile Networking Conference*, Paris, pp. 55-62, 2019.

[23] To T. and Duda A., "Simulation of LoRa in Ns-3: Improving LoRa Performance with CSMA," *in Proceedings of The International Conference on Communications*, Kansas City, pp. 1-7, 2018.

[24] Voigt T., Bor M., and Alonso J., "Mitigating Inter-network Interference in LoRa networks," *arXiv preprint arXiv:1611.00688*, 2016.

[25] Yang X., Karampatzakis E., Doerr C., and Kuipers F., "Security Vulnerabilities in LoRaWAN," *in Proceedings of IEEE International Conference on Internet-of-Things Design and Implementation*, Orlando, pp. 129-140, 2018.

[26] Zhou Q., Zheng K., Xing J., and Xu R., "Design and Implementation of Open LoRa for IoT," *IEEE Access*, vol. 7, pp. 100649-100657, 2019.

Ala' Khalifeh received the PhD degree in Electrical and Computer Engineering from the University of California, Irvine -USA in 2010. He is currently an Associate Professor in the Communication Engineering department at the German Jordanian University and the department chair. His research is in communications technology, and networking with particular emphasis on optimal resource allocations for multimedia transmission over wired and wireless networks, Quality of Service, Internet of Things and Wireless Sensor Networks.

Khaled Aldahdouh is a researcher in the Communication Engineering department at the German Jordanian University. He received the MSc degree in the Computer Engineering from the German Jordanian University in 2020, and the BA degree in the communication engineering from Philadelphia University in Jordan in 2017. His research is in wireless communications, 5G system, Internet of Things, and Wireless Sensor Networks based on LoRa technology.

Sahel Alouneh is a full professor of electrical and computer engineering. Currently, he is a member of the Cybersecurity program in Engineering College, Al Ain University, Abu Dhabi campus, in the UAE. His posts before joining Al Ain University, Prof. Alouneh held the post of the dean of Scientific Research at German Jordanian University (GJU) from October 2019 to August 2020. In addition, he served as the dean of the faculty of electrical engineering and information technology at the German Jordanian University (GJU) from September 2015 and September 2019. Prof. Alouneh also served as the vice dean of the deanship of graduate studies and scientific research at GJU from March 2014 to March 2015. He also served as the director of computer center at GJU from July 2009 to January 2012.