A Search into a Suitable Channel Access Control Protocol for LoRa-Based Networks

Muhammad Omer Farooq and Dirk Pesch

Nimbus Research Centre, Cork Institute of Technology, Cork, Ireland

Email: omer.farooq@cit.ie, dirk.pesch@cit.ie

Abstract—Low-power wide-area networking (LPWAN) has gained much attention recently and offers significant potential to support a large number of Internet of Things (IoT) applications. For device simplicity, LPWANs tend to use a simple channel access control protocol such as Aloha, which impacts performance. While several LPWAN technologies are available, we specifically focus on the Long Range (LoRa) in this paper. Our goal in this study is to search for a channel access control protocol in conjunction with the LoRa physical layer that can improve network performance in terms of reliability, throughput, energy consumption, and yet retain simplicity. We analyze a range of channel access control protocols, such as pure Aloha, delay before transmit, random frequency hopping, and carrier sense multiple access (CSMA). Our experiments use available periodic and event-based data traffic generation models for Internet of Things applications. Our results show that, CSMA and random frequency hopping demonstrate significantly better performance for both periodic and event-based data traffic models. Moreover, CSMA also exhibits scalability features in terms of the number of nodes in a network and data traffic generation models.

I. INTRODUCTION

The Internet of Things (IoT) promises to create an ecosystem of billions of connected devices to support a wide range of IoT applications [1]. Recently, many low-power wide-area radio technologies have emerged to support multitude of IoT applications, however Long Range (LoRa) [2] is the most popular radio technology. As the wireless communication medium is a shared medium, a protocol that governs how wireless nodes access the medium is of immense importance. A channel access control protocol can impact a network's reliability and energy consumption. For example, if a channel access control protocol allows a number of nodes to transmit data simultaneously, the transmitted data packets may collide, hence nodes may have to retransmit their data packets. Retransmissions result in higher energy consumption and latency, and waste bandwidth. An effective channel access control protocol is critical for low-power wide-area networks (LPWANs) as battery powered nodes require long lifetime and network bandwidth is rather limited. As LoRa/LoRaWAN is a relative new communication technology, much of the existing research has so far only focused on the LoRaWAN Aloha MAC. However, Aloha's scalability issues are well-known, and it has been shown that it does not satisfy performance requirements of many popular smart city use cases [3]. Therefore, there is a need for a study to analyze a range of simple and asynchronous channel access control protocols for LoRa-based networks considering important network performance metrics, such as reliability, throughput, and energy consumption.

We discuss and analyze suitability of different channel access control protocols for LoRa-based networks, such as pure Aloha, delay before transmit, random frequency hopping, and carrier sense multiple access (CSMA). The following are our main contributions: (i) implementation of delay before transmit, random frequency hopping, and CSMA channel access control protocols for LoRa in an existing LoRa simulator, (ii) performance analysis of different channel access control protocols for LoRa, and (iii) our results that demonstrate the following: among the evaluated protocols, multi-channel CSMA demonstrates significantly better reliability and energy consumption, and it demonstrates scalability features in terms of number of nodes in a networks and data generation traffic models.

The rest of this paper is organized as follows. Related work is discussed in Section II. The different channel access control protocols that were evaluated within a LoRa-based network are described in Section III. Our experimental study on the performance analysis of those channel access control protocols is presented in Section IV. Finally, conclusions are drawn in Section V.

II. RELATED WORK

LoRa is a physical layer radio modulation technique based on chirp spread spectrum (CSS). The goal is to enable low throughput communication across long distances with low power consumption. LoRa features include long range, multi-path resistance, robustness, low power consumption, forward error correction (FEC), and Doppler resistance. LoRa provides several physical layer parameters that can be customized. These parameters include spreading factor (SF), bandwidth (BW), transmission power (TP), and code rate (CR). These parameters affect the available bit rate, resilience against interference, and ease of decoding. LoRa uses seven different SFs, namely: $[SF6, SF7, SF8, SF9, SF10, SF11, SF12]$. In LoRa a transceiver can select a BW in the range [7.8, 500] kHz. However, LoRa transceivers typically operate at 125 KHz, 250 KHz, or 500 KHz. LoRa defines four different coding rates, $\frac{4}{5}$, $\frac{4}{6}$, $\frac{4}{7}$, and $\frac{4}{8}$. Higher CR implies higher protection against burst interference, and vice versa. LoRaWAN [2] is a MAC layer protocol and network architecture designed to be used with the LoRa physical layer. LoRaWAN uses pure Aloha

(PA) as a channel access protocol. A LoRaWAN gateway can decode eight simultaneous transmissions based on different combinations of SFs and BWs, however at any given time a node in a LoRaWAN network uses particular combination of SF, BW, TP, and CR.

LoRa throughput is analyzed in [4], [5], [6], and [7], which have primarily focused on Class A LoRaWAN devices. It has been shown that although LoRaWAN uses PA channel access control protocol, due to LoRa's robust modulation technique an increase of up to 1000 nodes per gateway results in only 32% more packet losses, whereas for the same scenario the losses are up to 90% in other PA-based networks [6]. As LoRa allows customization of transmission parameters, therefore recently some research efforts focused on devising algorithms for effective LoRa's transmission parameter selection by considering a specific goal. For example, in [8], a transmission parameter selection algorithm for LoRa is presented with a goal to minimize energy consumption at a specific reliability level. To enable LoRaWAN to achieve a high data rate two different spreading factor allocations algorithms are presented in [9]. Similarly, in [10] power and spreading factor control algorithm is presented to achieve fairness in LoRa-based networks.

Existing research work on LoRa has largely ignored the investigation of different channel access control protocols to improve the performance of LoRa in terms of reliability, throughput, and energy consumption. Therefore, here we focus on investigating the impact of a range of channel access control protocols on a LoRa-based network.

III. CHANNEL ACCESS CONTROL PROTOCOLS

A. Pure Aloha

Pure Aloha (PA) is the simplest channel access control protocol to share a communication medium. If a node has a data packet to transmit, it immediately transmits the data without sensing a communication channel. This implies that, if there is an ongoing transmission, the transmission of a data packet by another node results in a collision, hence it is likely that all nodes involved in the collision have to retransmit their data. Although, it is the simplest channel access control protocol, it is well-known that the protocol is neither efficient nor scalable. Nodes in a LoRaWAN network use this channel access protocol.

B. Delay Before Transmit

The delay before transmit (DBT) protocol for LoRaWAN networks has been proposed in [3]. The protocol proposes a systematic approach to delaying transmission of data packets. The protocol assumes that in a LoRaWAN network, nodes are assigned sequential IDs. The protocol uses a node's ID to calculate the amount of time the node has to wait before transmitting its data frame. At any node, the DBT (D_{BT}) is calculated as, $D_{BT} = (Node_{ID} \times U_d) \bmod Pkt_{iat}$. Here, $Node_{ID}$ is a node's ID, U_d is the delay in milliseconds (ms), and Pkt_{iat} is a node's mean packet inter-arrival time in ms. It is possible that a LoRa/LoRaWAN node does not buffer

frames, therefore to lower the packet drop probability, the DBT protocol uses $\bmod$ to limit D_{BT} to be within the mean packet inter-arrival time. Pkt_{iat} and U_d are configurable parameters. The values for these parameters depend on an application's requirements. In our experiments we use $U_d = 1000$.

C. Random Frequency Hopping

In LoRa-based networks, it is possible for a node to transmit a data packet by choosing a transmit frequency from a list of available transmit frequencies. If a LoRaWAN gateway a priori knows the set of available transmit frequencies, it can decode up to 8 simultaneous transmissions based on different transmit frequencies or LoRa communication settings. Moreover, there is no additional overhead to inform the gateway about the frequency that will be used to transmit a data packet. In current LoRaWAN MAC protocol implementation, the gateway uses special control message to instruct a node to switch to a different transmit frequency. Therefore, random frequency hopping (RFH) based MAC is different from LoRaWAN MAC as it does not require extra control message. In the RFH channel access mechanism, before transmitting each data packet, a node randomly selects a transmit frequency from the list of available transmit frequencies. Afterwards, a node uses PA protocol to transmit the data packet. As ETSI (European Telecommunications Standards Institute) 1% radio duty cycling rule applies to an individual channel, therefore RFH can also be used to support applications that require relative high throughput.

D. Carrier Sense Multiple Access

In CSMA, a node selects a transmit frequency from the list of available transmit frequencies, and senses the channel corresponding to the frequency for a specified duration of time. If there is no data activity on the channel, the data packet is transmitted. Otherwise, the node selects the subsequent transmit frequency, and repeats the sensing operation. If a communication medium is busy corresponding to each transmit frequency available in the transmit frequencies set, the node backs-off for a random number of time slots. The notion of a time slot is local to each node. The random time slot is selected from the contention window. The size of contention window is 2^N slots. Initially, $N = 1$ and it is incremented every time the node switches to back-off mode while trying to transmit the same data packet. After the data packet is transmitted or dropped N is reset to 1. Maximum value for N is the protocol's configurable parameter, and in our experiments the maximum value that N can take is 3. A data packet is dropped, if N becomes greater than 3, however assuming that typically LoRa nodes do not buffer packets, we consider that if $N \leq 3$ and a new data packet has arrived for transmission, the old data packet is dropped. As CSMA senses if the channel is free before a transmission, it allows a relaxation of the ETSI 1% duty-cycling rule, which is only strictly imposed on those channel access protocols that do not sense the channel before transmission.

In CSMA, a node has to calculate an appropriate duration for the time slot. As LoRa permits the use of different communication settings, and different settings result in different air time and the maximum application payload length that can be carried in the LoRaWAN frame, the CSMA channel access protocol's slot duration depends on the communication setting being used. In this study, we assume that nodes are using one of the recommended settings for LoRaWAN, i.e., BW = 125 KHz, SF = 12, and CR = 4/8. Based on this setting, the maximum application payload that can be carried in a LoRaWAN frame is 51 bytes. Therefore, the time required to transmit a single frame with the maximum application payload is 2466 ms [2].

IV. PERFORMANCE ANALYSIS

Here, we thoroughly analyze the suitability of the discussed channel access control protocols for LoRa-based networks. For the performance analysis we use the LoRaSim simulator [5]. The simulator only supports uplink traffic, therefore our analysis does not consider data frames that require an ACK from a gateway. In our experiments, 860 MHz transmit frequency is used, and we use one of the recommended settings for LoRaWAN, i.e., BW = 125 KHz, SF = 12, and CR = 4/8, along with the application payload length of 51 bytes. This is the maximum payload length that can be carried in a LoRaWAN frame with the mentioned LoRa setting. Hence, a slot duration of 2466 ms is used.

Our experiments are based on periodic and event-based data packet generation models. For periodic data generation, a data packet is generated every 30 minutes, and it is the recommended packet generation interval for a smart metering (SM) application [11]. For event-based data traffic, we target another popular smart city use case, i.e., a smart parking (SP) system. For a SP system, we use a data generation model reported in [12], which is based on extensive parking sensor readings from a deployment in a town in Northern Italy. The model is based on the Weibull distribution, to model parking duration and space occupancy the data generation model suggests the following values for different parameters of Weibull distribution: (i) parking duration $\lambda = 45.7422$ minutes, and $k = 0.6093$ and (ii) parking space occupancy $\lambda = 112.4832$ minutes, and $k = 0.8448$. A packet is transmitted to the gateway whenever a parking space becomes vacant or occupied.

A. Evaluation Metrics

As LoRaSim does not support downlink transmission, our evaluations are based on a target scenario, i.e., a simulation terminates after the gateway has successfully received 1000 packets from each node in a network, in other words for the simulation to terminate the gateway should receive $total\_nodes \times 1000$ packets. A node should not transmit packets once its 1000 packets have been successfully received at the gateway.

Transmit to Target Ratio (TTR): is the ratio of the total number of packets transmitted to achieve the target. $TTR =$ $\frac{Total\_transmissions}{total\_nodes \times 1000}$. The closer the value of TTR to 1 higher is a protocol's reliability and efficiency, and vice versa.

Network Total Energy Consumption (NTEC): The energy consumption model we use here is the same as reported in [5]. We report on NTEC that we assume is equal to the total energy consumed by the transceiver for all the nodes in a network. A transceiver consumes energy while transmitting, receiving, and sensing a channel. Therefore, energy consumed (E) by any LoRa node can be calculated as, $E = T_{tx}P_{tx} + T_{rx}P_{rx}$. $P_{tx} = 419.6\,mW$ and $P_{rx} = 44.06\,mW$ as given in LoRa SX1272 data sheet [13]. T_{tx} is the time spent in transmitting data, and T_{rx} is the time spent in receiving data. For the settings used in this study, the transmit consumption is 34 mA. Here, we assume that energy consumed in sensing is equivalent to the energy consumed in reception, therefore $T_{rx}P_{rx}$ is only relevant for the CSMA protocol. NTEC can be calculated by taking summation of the total energy consumption of each node in a network.

B. Experimental Results

Fig. 1(a) shows the TTR demonstrated by the different channel access control protocols using the SM data generation model. The PA protocol demonstrates the highest TTR, and the CSMA protocol demonstrates the lowest TTR amongst the evaluated protocols. Moreover, CSMA demonstrates scalability feature as with an increase in the number of nodes, the increase in the TTR is very low. The DBT protocol demonstrates up to 42% lower TTR compared to the PA protocol. Using the DBT protocol, it is likely that a number of nodes try to transmit at the same time, hence it demonstrates the second worst performance. RFH and CSMA demonstrate up to 55% and 81% lower TTR respectively compared to the PA protocol. In our experiments, RFH protocol selects the transmit frequency from the following set of frequencies: $860, 864, 868$ MHz. Therefore, using only two additional transmit frequencies along with the PA protocol demonstrates lower number of collisions, hence better TTR. Fig. 1(b) shows the NTEC demonstrated by the different protocols. PA demonstrates the highest NTEC, and despite of the fact that CSMA also consumes energy in channel sensing still it demonstrates the lowest NTEC, and it demonstrates up to 83% lower NTEC compared to PA. Similarly, RFH and DBT demonstrate up to 50%, and 38% lower energy consumption respectively compared to the PA protocol. Here, CSMA again demonstrates scalability in terms of energy consumption as with an increase in the number of nodes, the relative increase in NTEC is low.

Fig. 1(c) shows the TTR demonstrated by the channel access control protocols using the SP data generation model. Here, again PA demonstrates the highest TTR and CSMA demonstrates the lowest TTR. DBT, RFH, and CSMA demonstrate up to 6%, 34%, and 44% lower TTR respectively compared to the PA protocol. Comparison of Fig. 1(a) and Fig. 1(c) highlights the following point. Apart from CSMA protocol other evaluated protocols demonstrate significantly lower TTR using the SP data generation model. The reason is the data
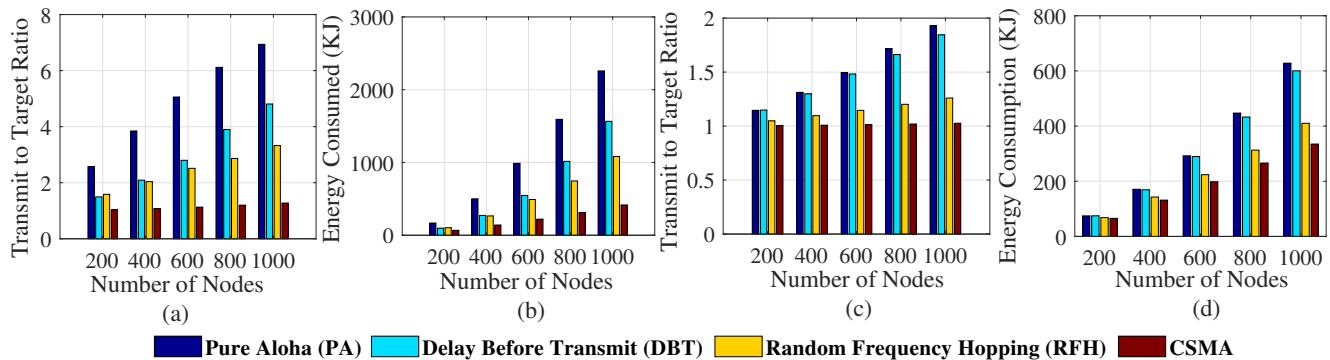
Fig. 1. MAC Layer Protocols' Performance Comparison

traffic generation model, i.e., in case of periodic traffic a number of nodes possibly try to transmit simultaneously, this results in a higher number of collision which leads to a higher TTR. Whereas, in the SP data generation model the probability of a number of nodes transmitting at the same time is relatively lower, hence lower collisions resulted in better TTR. Fig. 1(d) shows the NTEC demonstrated by the different channel access control protocols. DBT, RFH, and CSMA demonstrate up to 6.5%, 34%, and 48% lower energy consumption respectively compared to PA. Comparison of Fig. 1(b) and Fig. 1(d) highlights that NTEC in case of the SP data generation model is substantially lower than the NTEC demonstrated by the protocols in case of the SM data generation model. The number of transmissions in case of the SP data generation model is lower, hence the lower energy consumption.

C. Discussion

Despite of its simplicity the PA protocol demonstrates the highest TTR and energy consumption among the evaluated protocols. The CSMA is a little complex protocol, however our results demonstrate that the protocol is the best in terms of reliability, energy consumption, and scalability. Moreover, the sense before transmit feature of the protocol makes it an appropriate choice for IoT applications that require a high throughput, as the protocol is not restricted by ETSI's 1% duty cycling regulation. In situation, where CSMA cannot be used RFH is a simpler option with relatively good reliability, energy consumption, and scalability features.

V. CONCLUSIONS

We have analyzed a range of channel access control protocols for LoRa-based networks, namely: PA, DBT, RFH, and CSMA. For the purpose of our analysis, we implemented these protocols over the LoRaSim simulator. Our experimental studies used published periodic and event-based data traffic generation models for IoT applications. Our results demonstrated that among the evaluated protocols CSMA is scalable, and it has also shown the best performance in terms of reliability, throughput, and energy consumption. Our results also demonstrate the RFH is the second best channel access control protocol among the evaluated protocols after CSMA in terms of reliability and energy consumption. Therefore, in situation where CSMA cannot be used RFH can yield a good performance. The PA protocol demonstrated the poorest performance, hence it is not an appropriate protocol for LoRa-based networks.

REFERENCES

[1] S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, "A Global Perspective of Smart Cities: A Survey," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2013, pp. 439–444.

[2] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN Specifications, LoRa Alliance, San Ramon, CA, USA," 2015.

[3] M. O. Farooq and D. Pesch, "Analyzing LoRa: a Use Case Perspective," in *IEEE World Forum on the Internet of Things (WF-IoT)*, 2018, pp. 360–365.

[4] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the Limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[5] M. C. Bor, U. Roedig, T. Voigt, and J. 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*, ser. MSWiM '16, 2016, pp. 59–67.

[6] J. Haxhibeqiri, F. Van den Abeele, I. Moerman, and J. Hoebeke, "LoRa Scalability: A Simulation Model Based on Interference Measurements," *Sensors*, vol. 17, no. 6, 2017.

[7] K. Mikhaylov, . J. Petaejaejaervi, and T. Haenninen, "Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology," in 22th *European Wireless Conference*, May 2016, pp. 1–6.

[8] M. Bor and U. Roedig, "LoRa Transmission Parameter Selecction," in *Proceedings of Internation Conference on Distributed Computing in Sensor Systems*, ser. DCOSS '17, 2017.

[9] F. Cuomo, M. Campo, A. Caponi, G. Bianchi, G. Rossini, and P. Pisani, "Explora: Extending the Performance of LoRa by Suitable Spreading Factor Allocations," in *IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2017, pp. 1–8.

[10] B. Reynders, W. Meert, and S. Pollin, "Power and Spreading Factor Control in Low Power Wide Area Networks," in *IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[11] "Smart Meter Data Generation," https://www.energy-uk.org.uk/customers/about-smart-meters.html, last accessed: 16th March, 2018.

[12] N. Piovesan, L. Turi, E. Toigo, B. Martinez, and M. Rossi, "Data Analytics for Smart Parking Applications," *Sensors*, vol. 16, no. 10, 2016.

[13] "Semtech SX1272," https://www.semtech.com/apps/product.php?pn=SX1272, last accessed: 16th March, 2018.