On the Use of Carrier Sense Mechanisms in Low-Power Wide Area Networks

Abderrahman Ben Khalifa, Razvan Stanica, Hervé Rivano
Univ Lyon, INSA Lyon, Inria, CITI, F-69621 Villeurbanne, France
Email: abderrahman.ben-khalifa@insa-lyon.fr

Abstract—**Adding carrier sense capabilities to nodes in low-power wide area networks is considered as a good strategy to cope with scalability problems. However, in settings with large cells, the clear channel assessment function will give imperfect results, producing scenarios rich in hidden nodes. In this paper, we assess the impact of these hidden nodes, showing that the average gains with respect to an Aloha strategy are significantly decreasing as the number of hidden nodes increases. Moreover, in terms of energy, our results indicate that carrier sensing consumes 10 to 100 times more than a simple Aloha channel access. We also look at the individual node behavior, demonstrating an important heterogeneity among nodes, with performance generally correlated to the quality of the carrier sense mechanism.**

I. INTRODUCTION

The increasing interest in connected objects resulted in the design of dedicated technologies for the access to the Internet of Things (IoT). Also known as low-power wide area networks (LPWANs), these technologies, in the likes of Sigfox [1] or LoRa [2], take a cellular-based approach, with radio towers covering large areas (in the order of tens of kilometers) and potentially hundreds of thousands of communicating objects. However, the network traffic pattern in LPWANs is very different from the one in classical cellular networks. The connected objects are expected to transmit mostly uplink data to the radio gateway, and further on to application servers [3].

From a channel access perspective, the problem is also very different. Connected objects are expected to produce short messages in periodic or event-driven manner, resulting in massive IoT scenarios [4]. The overhead required by centralized cellular uplink scheduling [5] is prohibitive for the energy-constrained objects. Therefore, all LPWAN technologies took a distributed approach at the medium access control (MAC) layer, based on the well-known Aloha protocol [6].

Practically, in Aloha, the MAC layer transmits the message on the channel as soon as possible, without any prior coordination with other stations. In case an acknowledgement (ACK) message is not received, the MAC layer retransmits the original message, after a random back-off time. This procedure is slightly modified in LPWANs, where the downlink is highly limited: each message is automatically retransmitted several times, following a random process, without waiting for ACKs. Known for its simplicity, Aloha also has well-documented performance issues, especially in terms of scalability [7]. To address this challenge, LPWAN technologies propose to increase the space used by the Aloha random process by using an extra dimension, not only the temporal one. For example, Sigfox uses time and frequency, while LoRa uses the time and code dimensions. However, it is clear that this simply pushes the bottleneck of the protocol, without solving its core issues.

Recent studies proposed adding carrier sense capabilities to LPWAN nodes to improve network scalability [8], [9], [10], [11]. Carrier sense multiple access (CSMA) is already successfully used in wireless local area networks (WLAN), so it seems a straightforward choice for IoT networks as well. However, LPWANs are highly asymmetrical, in the sense that radio gateways are powerful, carefully designed receivers, while IoT nodes usually include cheap, low-end radios. Considering that a radio gateway can cover very large areas, it seems highly unrealistic to consider, like the studies cited above, that IoT nodes can sense all their contenders during the channel access procedure. It is more likely that adding carrier sense in a LPWAN will create scenarios rich in hidden nodes [12], degrading the efficiency of CSMA.

The contribution of this paper is the study of the CSMA clear channel assessment (CCA) function in LPWANs, under realistic settings. In this sense, we define a new metric, denoted as CCA conflict rate, and we observe through simulation its evolution for different levels of receiver sensitivity. We show that, while a perfect carrier sense mechanism can indeed bring significant improvements over Aloha in terms of packet success probability (PSP), the gains are much lower when hidden nodes are considered. Moreover, the energy cost needed by the carrier sense mechanism is important, between 10 and 100 times the one of Aloha on average. We also look at individual node behavior, showing a significant heterogeneity among nodes. Interestingly, the MAC performance does not depend on the absolute value of the CCA conflict rate, but a relative correlation is apparent in most scenarios.

II. RELATED WORK

CSMA is a widely used solution at the MAC layer, mainly used by the IEEE 802.11 standard for WLANs. In this context, the performance of CSMA has been extensively studied [13] and compared with Aloha [14]. The impact of the receiver sensitivity, modelled through the CCA threshold parameter has also been studied, in different scenarios, such as mesh networks [15] or vehicular networks [16]. However, LPWANs represent a significantly different scenario: the traffic is mostly uplink, the MAC layer is not saturated and, most importantly, ACK messages are not used on the downlink. Current

LPWANs use an Aloha-based MAC layer, with well known scalability limits [17].

For this reason, several studies proposed enhancing dedicated IoT networks with carrier sensing [8], [9], [10], [11]. Pham [8] and Kouvelas *et al.* [9] added a carrier sense mechanism to LPWAN devices by exploiting the channel activity detection procedure present on LoRa devices. Pham [8] experimentally shows how CSMA adds robustness with respect to collisions in a LoRa network. Similar properties are demonstrated through simulation by To *et al.* [10]. Moreover, this latter study shows that using a non-persistent CSMA approach results in an energy consumption close to the one obtained by Aloha. Taking the opposite approach, Kouvelas *et al.* [9] study a persistent CSMA MAC solution, also in LoRa networks. The authors show that their approach decreases the number of collisions and enables the detection of interferers. Finally, Zucchetto *et al.* [11] show the superiority of the *listen before talk* approach used in CSMA in terms of PSP.

All the aforementioned contributions consider a perfect carrier sense mechanism, where every node in the network is able to sense all its contenders, when CSMA is enabled. We consider this to be highly unrealistic in LPWANs, where cheap receivers are used on the nodes side and the cells are very large (in the order of kilometers). Our previous work [18] considered an imperfect carrier sense range for IoT devices, but in the context of an ACK based protocol, such as WiFi HaLow [19]. We extend this work here, by considering LPWANs and a MAC layer where ACK messages are not transmitted, because of downlink limitations.

III. EVALUATION METHODOLOGY

We use the Network Simulator 3 (ns3) to study a LPWAN with N connected objects and one radio gateway. Practically, we build a network topology consisting of a single cell, with a gateway node situated in its center. The IoT nodes are uniformly distributed inside this area and they all share the same channel. Each sender node produces one packet of data each time period T and passes it to the MAC layer for transmission. The gateway node only acts as a receiver and it does not transmit any ACK frames, in line with LPWAN technologies. To add robustness at the MAC layer without using ACKs, the IoT nodes systematically retransmit each packet K times (from 1 to 3 times in our study).

Different IoT technologies achieve very different data rates at the physical layer. This depends on several physical layer parameters, such as modulation, coding, spreading factor, etc. In order to have a fair, but technology agnostic comparison, we use as a parameter the *transmission opportunity*, $T_{op} = S/T$, where S is the airtime of a MAC layer frame. As an example, a T_{op} value of $165 \cdot 10^{-6}$ would correspond to a packet arrival every 20 minutes in Sigfox.

For performance evaluation, we use two metrics that we consider relevant in LPWANs: the PSP (i.e. the correct reception of at least one of the K retransmissions) and the time duration spent by each node in an active state (receiving, transmitting or listening to the channel, denoted as ON state). We believe that this second metric is a good generic proxy for the energy consumption of a node and we use it instead of a more classical metric, which would require the use of technology-specific parameters.

To simulate the CSMA protocol, we use the ns3 AdhocWifiMac model, where the CCA threshold is set by default at -99 dBm. However, as explained below, we test different values for this parameter in our study. Practically, by varying the CCA threshold, we simulate receivers with different sensitivities. For example, cheaper receivers would have a lower sensitivity, hence a higher CCA threshold. By default, the AdhocWifiMac model in ns3 uses ACK messages to confirm frame reception. We deactivate this mechanism and transmit each packet K times. The time between consecutive retransmission attempts of the same packet is randomly selected between 0 and $T/10$. Of course, the MAC layer will further delay the retransmission if the channel is detected as busy.

We run simulations while varying the number of sender nodes. Every simulation lasts 30 seconds and it is repeated 10 times, with a different seed value each time. All the results presented in the remainder of the paper that show average values are given with a confidence interval of 95%.

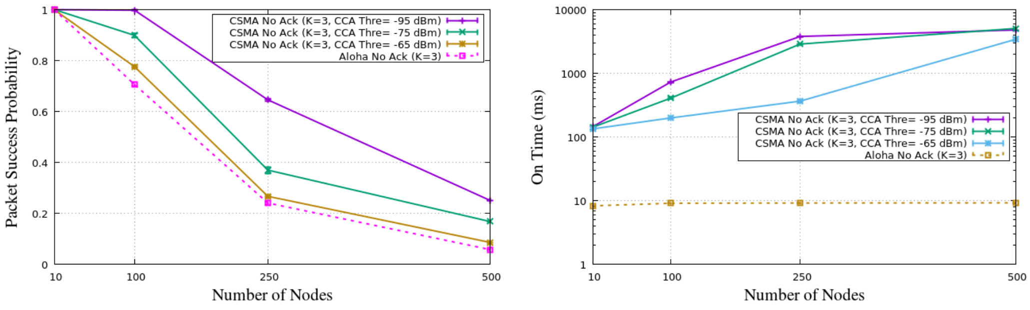
IV. GENERAL OBSERVATIONS

In this section, we study the impact of the CCA threshold on the CSMA protocol in a LPWAN context, by evaluating the average PSP and the average time spent by the nodes in an ON state.

A. Packet Success Probability

Since we are interested in the general performance of the MAC layer, in Fig. 1a we present the average packet success probability of the CSMA protocol, calculated for different numbers of contending nodes and different values of the CCA threshold. In order to measure the efficiency of the CCA technique we show in the same figure the results obtained by the Aloha protocol. In these results, for both protocols (denoted as CSMA No Ack and Aloha No Ack), the number of retransmissions is set at $K = 3$, a value commonly used in LPWANs. We remind the reader that increasing the CCA threshold is equivalent to reducing the receiver sensitivity. Therefore, if the CCA threshold is very high, the carrier sense mechanism has no effect and CSMA should behave identically to Aloha in this case.

We can see from the simulation results that the average PSP in the network depends on the value of the CCA threshold parameter. It is clear that, for the lowest value of -95 dBm, we get the best performance, since the node sensitivity is very high. As we will see later on, in this case the carrier sense range of a node covers the entire cell, removing any impact from hidden nodes. This is the classical scenario considered in the related work. Indeed, the results show the same impressive gains found in previous studies [8], [10] when carrier sense is added. In our study, CSMA with a perfect CCA threshold (-95 dBm) reaches a PSP 40% higher than Aloha for the case of 250 nodes, representative of a medium loaded LPWAN.



(a) Packet Success Probability

(b) On Time (ms).

Fig. 1. CSMA and Aloha packet success ratio and ON time.

However, these observations radically change when the CCA threshold increases (equivalent to a lower receiver sensitivity). For example, the gain for CSMA with a CCA threshold of -75 dBm is only 20% with respect to Aloha. If we further increase the value of this parameter, to -65 dBm, the results become very close to those obtained by an Aloha strategy.

To summarize, our results indicate that the gains brought by CSMA in LPWANs are largely overestimated by previous studies. While the gains are indeed significant for receivers with a high sensitivity, low-end IoT receivers do not perform much better using CSMA instead of Aloha.

B. Activity Time

As explained in Sec. III, in this work we do not directly compute the node energy consumption, as this would require a technology-specific energy model. Instead, we calculate a correlated metric, the duration each node spends in an active ON state, i.e. the time the node is using its radio module, either for transmission, reception or listening the channel. Fig. 1b shows the average ON time of the network, for the CSMA and Aloha protocols and for different node densities. The results for the CSMA solutions show that the lower the CCA threshold, the higher the observed ON time period. This is due to the larger sensing areas achieved by the IoT nodes when their sensitivity is high. In this case, the nodes spend more time sensing the channel and waiting for it to become free (i.e. the duration of the back-off periods is longer).

We can notice that the CCA threshold values of -95 dBm and -75 dBm result in similar ON time periods for medium (250 nodes) and high (500 nodes) density networks. Using a CCA threshold of -65 dBm gives the best energy results in a medium density network, but almost catches up with the other CSMA flavors in high density networks, as the numerous close neighbors still trigger increased back-off periods.

On the other side, Aloha results in much better results from an energy point of view. The average ON time when using Aloha is 10 times lower than CSMA in a low density scenario, and more than 100 times lower in a high density scenario. In fact, the Aloha ON time is constant, since in this case the nodes are awake only for transmissions, and the number of packets generated by each node is independent from the network density.

If we consider the PSP and the ON time results together, we can say that CSMA is indeed better than Aloha in terms of PSP when the receiver sensitivity is high (i.e. low CCA threshold). But this comes with the price of an increased ON time, hence a higher energy consumption, which is not a very welcomed property in many IoT applications. Still, in ideal conditions, a 40% increase in PSP might be worthy this increased energy consumption. However, when the CSMA protocol is functioning on devices with a reduced receiver sensitivity, the PSP is only slightly higher than the Aloha one, while the ON time is much larger. In this case, it is hard to find any interest in using CSMA.

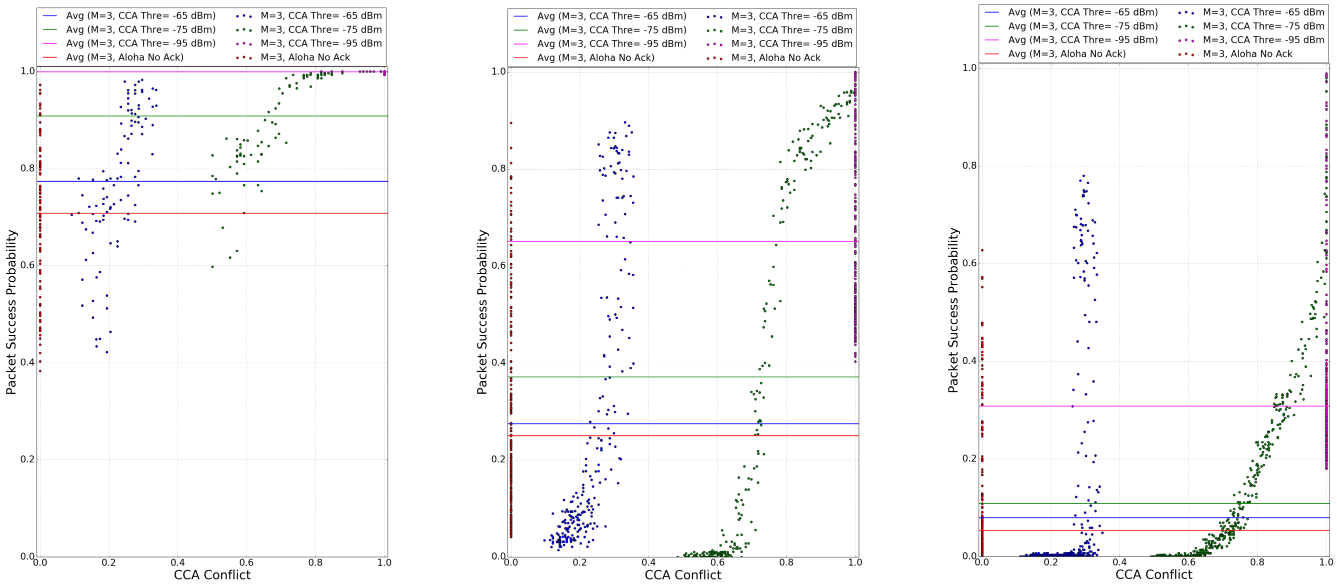
V. OBSERVATIONS AT INDIVIDUAL LEVEL

In this work, we argue that it is not realistic to consider that an IoT node senses all the other nodes in a large LPWAN cell. By changing the CCA threshold of the nodes, we can model this phenomenon, where only a part of the transmissions towards the gateway can be sensed by each individual device. Indeed, depending on their position in the network and on their CCA threshold, nodes can have a certain number of hidden interferers, a phenomenon well known in the literature [20].

To assess the impact of the hidden terminals in our network, we define a metric denoted as the CCA conflict rate. This metric is computed for each node and it shows the ratio of nodes in the cell with which the considered node is in conflict. In other words this metrics gives the ratio of nodes in the cell that are in the CCA detection zone of the considered node. The CCA conflict rate depends directly on the value of the CCA threshold and it is calculated for a node A as follow:

$$CCA\_CR_A = \frac{1}{(N-1)} \sum_{i \in N \setminus \{A\}} \frac{Rx_i^A}{Tx_i} \tag{1}$$

where Rx_i^A represents the number of frames overheard by node A from the total Tx_i frames transmitted by node i. Our goal is to measure the number of contenders of node A, while also accounting for the probabilistic nature of the radio propagation model. Indeed, in some cases, only a part of the messages transmitted by i actually activate the carrier sense mechanism of node A, and this definition allows considering these situations.



(a) 100 nodes.

(b) 250 nodes.

(c) 500 nodes.

Fig. 2. Individual node PSP and CCA conflict rate for different CCA threshold values, and for Aloha

A. Packet Success Probability

In Fig. 2, we show the PSP obtained by each individual node in the network, as well as its CCA conflict rate. We also show the average PSP in the network through horizontal lines. We notice that, in all network densities, the average PSP drops when the CCA conflict rate decreases. This is expected, since low CCA conflict rates imply a high number of hidden terminals. We also notice that there is a sort of a correlation between the relative CCA conflict rate of the nodes and their PSP results, a property more visible in the case of a CCA threshold of -75 dBm (green dots), but also present for a CCA threshold of -65 dBm (blue dots). For a CCA threshold of -95 dBm (pink dots), no such correlation is observed, since all the nodes of the network have the same CCA conflict rate value of 1, meaning that no hidden nodes exist in this scenario.

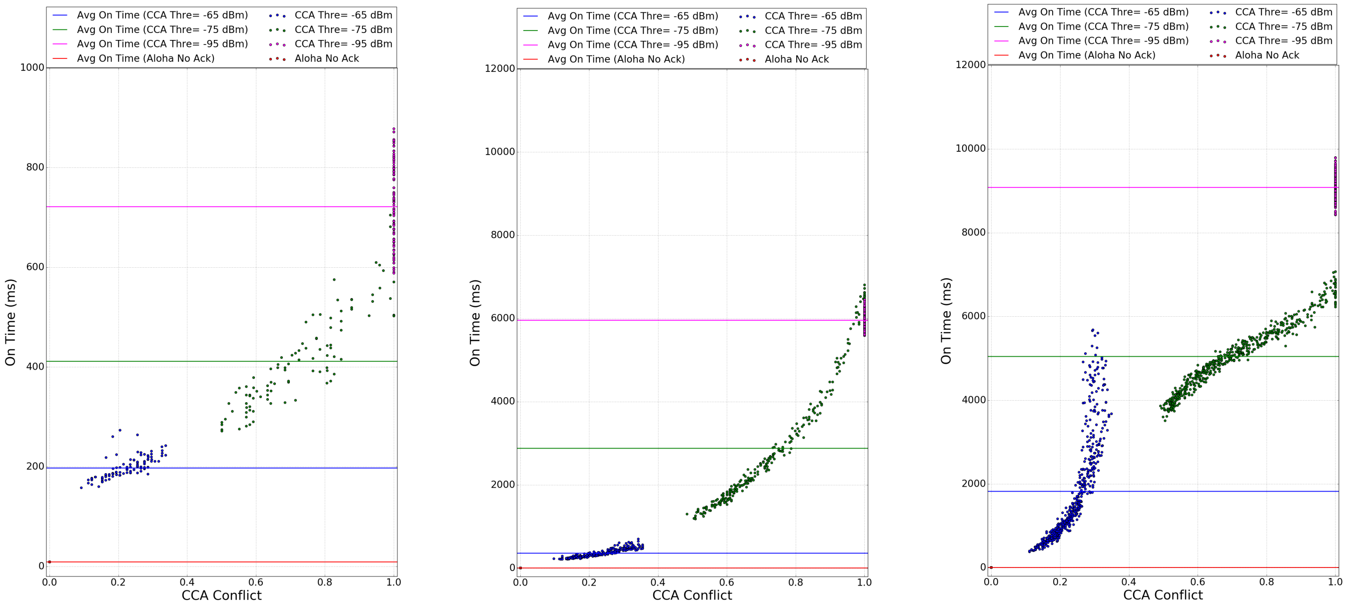
We note that the correlation discussed above does not hold for the absolute values of the CCA conflict rate, but only for the relative values in each scenario. Indeed, a node with a CCA conflict rate of 0.4 among the blue dots attains a better PSP than a node with a CCA conflict rate of 0.6 among the green dots. This implies that the important factor is not the CCA conflict rate per se, but the differences in terms of CCA conflict rate among nodes. We note that such differences should be common in real scenarios, with IoT devices produced by different manufacturers, hence with different receiver sensitivities.

We also observe a significant heterogeneity in node performance. Indeed, while some nodes obtain a PSP close to 1, others are close to 0. This phenomenon was hidden by the average values presented in Fig. 1. These results indicate that fairness needs to be considered as a potentially important issue in CSMA-based LPWANs. Realistically, we consider that the two higher values of the CCA threshold (-75 dBm and -65 dBm), which show the most important heterogeneity in terms of PSP, are the closest to a real-world IoT network. It is important to note that Aloha-based solutions also present a similar heterogeneity in terms of individual node PSP.

B. Node Activity Time

Fig. 3 depicts the relationship between the individual CCA conflict rate and the node ON time. In this case, the correlation seems to hold for the absolute CCA conflict rate value: the more contenders a node has, the higher its energy costs when CSMA is used. Some exceptions exist, for example a few blue nodes in the high density scenario, which have a high energy consumption. The reason for this is that the scenario in question also contains some nodes with a very low CCA conflict rate (below 0.1). These nodes have a behavior close to Aloha. Since they are very aggressive and never back-off, they block the transmissions of more sensitive nodes and keep them ON for longer times. Just as in the case of PSP, the heterogeneity among nodes can be significant. In all the scenarios, the nodes with a higher receiver sensitivity consume much more energy than others.

Observing the individual PSP and ON time results together, we can conclude that the nodes with the best sensitivity in a LPWAN can reach a significant gain in terms of PSP with respect to their contenders. This comes indeed with the price of increased energy consumption, but paying this price might be worth for the nodes with the top CCA conflict rate. For the other nodes, activating the carrier sense mechanism seems rather counter-productive.



(a) 100 nodes.

(b) 250 nodes.

(c) 500 nodes.

Fig. 3. Node energy consumption and CCA conflict rate for different CCA threshold values, and for Aloha.

VI. CONCLUSION

The idea of adding carrier sense capabilities to LPWAN nodes is gaining popularity lately. However, previous studies only consider perfect scenarios, where the carrier sense range of a device covers all the contenders. In this paper, we investigate the impact of an imperfect carrier sense function, when only a subset of the contenders can be sensed. Our results show that the performance of a CSMA approach in LPWANs drastically drops in this realistic scenarios, and only the devices with the highest receiver sensitivity might take benefits from the carrier sense mechanism.

ACKNOWLEDGMENT

This work has been partly supported by the INSA Lyon - SPIE ICS chair on the Internet of Things.

REFERENCES

[1] Y. Mo, C. Goursaud, J.M. Gorce. "Theoretical Analysis of UNB-based IoT Networks with Path Loss and Random Spectrum Access", *Proc. IEEE PIMRC 2016*, Valencia, Spain, Sep. 2016.

[2] O. Iova, A.L. Murphy, G.P. Picco, L. Ghiro, D. Molteni, F. Ossi, F. Cagnacci, "LoRa from the City to the Mountains: Exploration of Hardware and Environmental Factors", *Proc. MadCom 2017*, Uppsala, Sweden, Feb. 2017.

[3] A. Sivanathan, D. Sherratt, H.H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman, "Characterizing and Classifying IoT Traffic in Smart Cities and Campuses", *Proc. IEEE Infocom SmartCity 2017*, Atlanta, GA, USA, May 2017.

[4] V. Gupta, S.K. Devar, N.H. Kumar, K.P. Bagadi, "Modelling of IoT Traffic and its Impact on LoRaWAN", *Proc. IEEE Globecom 2017*, Singapore, Singapore, Dec. 2017.

[5] Y. Ozcan, C. Rosenberg, "Efficient Loss-Aware Uplink Scheduling", *Proc. IEEE WCNC 2018*, Barcelona, Spain, Apr. 2018.

[6] F. Tobagi, "Analysis of a Two-Hop Centralized Packet Radio Network - Part I: Slotted ALOHA", *IEEE Transactions on Communications*, vol. 28, no. 2, pp. 196–207, Feb. 1980.

[7] A. Ben Khalifa, R. Stanica, "Performance Evaluation of Channel Access Methods for Dedicated IoT Networks", *Proc. IFIP WD 2019*, Manchester, UK, Apr. 2019.

[8] C. Pham, "Robust CSMA for Long-Range LoRa Transmissions with Image Sensing Devices", *Proc. IFIP WD 2018*, Dubai, UAE, Apr. 2018.

[9] N. Kouvelas, V.S. Rao, R.V. Prasad, G. Tawde, K. Langendoen, "p-CARMA: Politely Scaling LoRaWAN", *Proc. EWSN 2020*, Lyon, France, Feb. 2020.

[10] T.-H. To, A. Duda, "Simulation of LoRa in NS-3: Improving LoRa Performance with CSMA", *Proc. IEEE ICC 2018*, Kansas City, MO, USA, May 2018.

[11] D. Zucchetto, A. Zanella, "Uncoordinated Access Schemes for the IoT: Approaches, Regulations, and Performance", *IEEE Communications Magazine*, vol. 55, no. 9, pp. 48–54, Sep. 2017.

[12] C.L. Fullmer, J.J. Garcia Luna Aceves, "Solutions to Hidden Terminal Problems in Wireless Networks", *ACM SIGCOMM Computer Communication Review*, vol. 27, no. 4, pp. 39–49, Oct. 1997.

[13] T. Begin, B. Baynat, I. Guerin Lassous, T. Abreu, "Performance Analysis of Multi-Hop Flows in IEEE 802.11 Networks: A Flexible and Accurate Modeling Framework", *Elsevier Performance Evaluation*, vol. 96, no. 2, pp. 12–32, Feb. 2016.

[14] M. Kaynia, N. Jindal, "Performance of ALOHA and CSMA in Spatially Distributed Wireless Networks", *Proc. IEEE ICC 2008*, Beijing, China, May 2008.

[15] X. Yang, N. Vaidya, "On Physical Carrier Sensing in Wireless Ad Hoc Networks", *Proc. IEEE Infocom 2005*, Miami, FL, USA, Mar. 2005.

[16] R. Stanica, E. Chaput, A.-L. Beylot, "Physical Carrier Sense in Vehicular Ad-Hoc Networks", *Proc. IEEE MASS 2011*, Valencia, Spain, Oct. 2011.

[17] Q. Song, X. Lagrange, L. Nuaymi, "An Analytical Model for S-ALOHA Performance Evaluation in M2M Networks", *Proc. IEEE ICC 2017*, Paris, France, May 2017.

[18] A. Ben Khalifa, R. Stanica, "CCA Threshold Impact on the MAC Layer Performance in IoT Networks", *Proc. IEEE VTC Spring 2020*, Antwerp, Belgium, May 2020.

[19] T. Adame, A. Bel, B. Bellalta, J. Barcelo, M. Oliver, "IEEE 802.11ah: The WiFi Approach for M2M Communications", *IEEE Wireless Communications Magazine*, vol. 21, no. 6, pp. 144–152, Dec. 2014.

[20] L.B. Jiang, S.C. Liew. "Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks", *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 34–49, Jan. 2008.