Jamming Resilient Multi-Channel Transmission for Cognitive Radio IoT-based Medical Networks

Monette H. Khadr, Haythem Bany Salameh, Moussa Ayyash, Hany Elgala, and Sufyan Almajali

***Abstract*—The era of the Internet-of-things (IoT) comes with tremendous burdens on pre-existing network infrastructures and protocols due to spectrum scarcity and reliability concerns. Cognitive radio (CR) technology is proposed for IoT applications to alleviate the spectrum scarcity paradigm. In CR-IoT-based networks, the IoT devices/nodes share the spectrum with primary users (PUs). However, in order not to interfere with PUs communications and to conform with the elevating throughput requirements, efficient multi-radio/multi-channel assignment algorithms are required. Additionally, in order to ensure reliable transmission, algorithms need to be resilient to jamming attacks, which have detrimental impacts on network performance. In this paper, parallel-channel security-aware medium access control (PCS-MAC) is proposed as a probabilistic-based jamming resilient multi-channel assignment algorithm proposed for medical networks. PCS-MAC considers primary user activity, channel conditions, jamming attack levels, and data-rate requirements to provide spectrally efficient data transmission between CR-IoT nodes subject to delay constraints under jamming attacks to assure the delivery of time-critical patient data. The performance of PCS-MAC is practically validated using the open large-scale future Internet-of-things (FIT) IoT-LAB testbed. Practical results show that our proposed algorithm significantly enhances network performance, yielding throughput rates that supersedes the state-of-the-art algorithms presented in literature.**

***Index Terms*—Cognitive radio, Internet-of-things, jammer, security, spectrum assignment, testbed.**

I. Introduction

THE Internet landscape is burgeoning, especially now with the introduction of a multitude of devices that are connected to the Internet [1]. Internet-of-things (IoT) is the technology that encompasses the enormous range of devices that can connect to the Internet and require sharing data with other neighbouring devices [2]. Due to the interconnected nature of IoT devices, even a single poorly secured device or service can be an entry point for a cyber attack and potentially affect the security and resilience of the Internet globally [3]. Moreover, these IoT devices can carry time-critical information, such as in healthcare and disaster response applications, which can be life threatening if not received in a timely fashion. Jamming attacks can obstruct transmission either by damaging ongoing packets or denying devices from accessing the shared wireless channel. Since jamming attacks are considered the most common type of attacks in wireless networks [4], jamming resilient algorithms are crucial in IoT networks. Cognitive radio (CR) technology is presented as a solution for IoT-based networks to improve spectrum utilization by allowing dynamic spectrum access [5], [6]. In CR-IoT-based networks, IoT devices share the wireless channel with nodes that act as licensed primary users (PUs). IoT devices, on the other hand, act as unlicensed secondary users (SUs) and are granted access to the spectrum as long as they do not interfere with PUs transmissions. As IoT-based applications are becoming more integrated and pervasive in our daily lives, the reliability of their transmissions is vital. Additionally, with the uprise of new applications, such as remote-telesurgery, throughput requirements are becoming stringent and dynamic. The key lies in finding an efficient approach to utilize idle channels in CR-IoT-based networks while mitigating jamming attacks and satisfying quality-of-service (QoS) requirements. Due to the aforementioned reasons, a channel-assignment algorithm that is jamming resilient and allows multi-channel transmission while serving different QoS requirements is significantly crucial, especially in medical networks.

A. Background and Related Work

There are a vast number of approaches proposed for handling jamming attacks in CR-based networks. Jamming might result in a denial-of-service (DoS) attack, which is one of the most serious and challenging security attacks in CR networks [7]. Anti-jamming approaches include jamming detection, prevention, and mitigation. The intuition behind detecting jamming attacks is very basic; as the presence of jamming signals at the receiver's end most probably affects the received signal strength [8]. However, correct jamming detection is difficult based on a single system parameter [9], as it causes inaccurate classification. Other parameters such as packet-send-ratio, packet-delivery-ratio, and carrier-sensing-time can be incorporated to model jamming detection systems. Machine learning methods are now proving its efficacy to

Manuscript received October 29, 2021 revised June 17, 2022; approved for publication by Jiming Chen, Division 2 Editor, September 27, 2022.

This work was supported in part by ASPIRE Award for Research Excellence (AARE) 2020, Abu Dhabi, UAE, Grant number AARE20–161.

A limited subset of initial results was preliminarily presented at the IEEE Global Communications Conference (GLOBECOM), HI, USA, 2019.

M. H. Khadr and H. Elgala are with the Electrical and Computer Engineering Department, University at Albany, USA, emails: {mkhadr, helgala}@albany.edu.

H. Bany Salameh is with the Department of Network & Communications Engineering, Al Ain University, UAE, and also with the Department of Telecommunications Engineering, Yarmouk University, Jordan, email: haythem.banysalameh@aau.ac.ae.

M. Ayyash is with the Department of Computing, Information, and Mathematical Sciences and Technology, Chicago State University, USA, email: msma@ieee.org.

S. Almajali is with the Computer Science Department, Princess Sumaya University for Technology, Jordan, email: s.almajali@psut.edu.jo.

M. H. Khadr is the corresponding author.

Digital Object Identifier: 10.23919/JCN.2022.000042

1229-2370/22/$10.00 © 2022 KICS

provide lightweight detection of jamming attacks such as in the work done in [10], [11]. An influential work on jamming attacks modeling, evaluation, and detection can be found in [12], which is considered the foundation of the analysis in this paper and will be thoroughly detailed in Section II.

For jamming prevention, a honeynet-based defense mechanism is proposed in [9], which aims to avert the attacker from jamming genuine communications. This is accomplished by dedicating a node, named honeynode, to gather data and behavior from cyber attacks. The honeynode acts as a decoy as the jammer intensifies its attack toward it, thus, reducing the attack on the remaining nodes. Game theory recently emerged as a framework for addressing jamming in CR networks. Amin *et al.*, in [13], investigated a game theoretical model that aimed to maximize the utility of CR nodes in the presence of intruders and jammers. In the analysis, CR nodes are assumed to know the positions of the jammers and each others, which is an assumption that can be troublesome in practical deployment. Rawat *et al.* extended the work done in [13] to include primary user emulation (PUE) attacks in [14]. Similarly, the location of the PU and CR nodes were shared among the nodes and a spectrum sensor was utilized. The sensor used signal energy and bandwidth, cyclostationary features, and location verification techniques to identity channel status. The aforementioned methods, among others, either relied on dedicated nodes or additional hardware elements for sensing, which is again intensive for IoT-based networks.

Adopting multi-radio/multi-channel transmission in IoT-based networks is a novel field of research and is still in its early stages. This field is grabbing attention as the requirements of future IoT networks are evolving and the demands for increased data-rates are increasing. The work in [15] is dedicated to a multi-channel assignment algorithm that aims to reduce inter-channel interference, and then the work was extended to include various quality-of-service (QoS) requirements in [16]. A multi-channel cluster tree for beacon-enabled IEEE 802.15.4 wireless sensor networks was presented in [17] to minimize beacon collisions. Another multi-channel medium access control (MAC) protocol for IoT that took into account channel conditions, latency and frame reception ratio can be found in [18]. An online learning method based on Dirichlet process in [19] is investigated for multi-user multi-channel scenario in cognitive radio networks. Moreover, a Q-learning based spectrum access scheme is proposed for CR networks in [20]. However, mitigating jamming for such networks remains an unexplored field of research.

Given the decentralized nature of most IoT deployments, the majority of the presented parallel-channel (i.e., multi-channel) assignment techniques base their decisions on a per-link sequential greedy method without considering other nodes (i.e., other CR users). The objective of this work is to service the QoS requirements of the multi-channel/multi-radio CR-IoT nodes while utilizing the least amount of channels possible in order to provide a fair and non-greedy utilization of the network resources (i.e., spectrum) even in the absence of an IoT controller. Hence, high complexity (i.e., have multi-channel/multi-radio capabilities) IoT devices can coexist with low complexity devices. Additionally, our proposed algorithm addresses jamming attacks at the device level while considering channel conditions, PU activity, and delay requirements without additional dedicated nodes or hardware requirements (i.e., additional sensors). Perhaps, the analysis that is closest to our approach is the MAX-PoS approach proposed in [21], [22]. The fundamental difference, however, is that MAX-PoS only considers channel conditions and PUs activities, but it is impervious to jamming. Security-aware MAC, presented in [23], also addressed the aforementioned considerations, however, it was limited to a single-channel configuration.

B. Our Contribution

This paper introduces a parallel-channel security-aware medium access control (PCS-MAC) for CR-IoT-based networks as a jamming resilient, service oriented, multi-channel assignment algorithm designed to satisfy high-data requirements of cutting edge IoT applications. The focus of this paper is highly-reliable delay-sensitive CR-IoT networks; i.e., IoT networks equipped with CR capabilities, used for highly-reliable delay-sensitive applications (e.g., healthcare, military, indoor monitoring, etc.) [23]–[25]. The main feature of these networks is that, while they employ the CR technology to provide the spectrum needed for interconnecting large numbers of IoT devices, the CR technology itself raises a challenge against achieving the required high packet success probabilities. In particular, the PU activity and jamming attacks are considered the main source of packet failures, since a given transmission over a certain set of channels can be interrupted by PU transmissions or jamming attacks. Therefore, there is a need for channel assignment algorithms designed for achieving low packet failure probabilities, while taking into consideration the PU activities, and jamming attacks.

The proposed algorithm also has several applications in medical networks. This includes applications that require high mobility of patients with a minimum delay of data delivery to the right targets. Applications include IoT-based remote patient monitoring systems. Several patient health readings (e.g., blood pressure, heart rate, etc) can be read via wearable IoT devices and reported back to physicians and hospitals on a real-time basis. The sensitivity of the delay is very high in such applications as emergency cases might require physicians to take immediate actions. The mobility of a large number of patients along with the continuous small-size messages required by such applications make our CR-based algorithm a perfect efficient solution for bandwidth utilization. Similarly, IoT based Parkinson patient monitoring applications allow remote tracking of the footsteps of moving patients, detection of abnormal steps and timely reaction. Also, tracking the location of Alzheimer patients can be done via IoT-based insoles with built-in GPS capabilities.

The algorithm aims to enhance the overall network performance by selecting the least number of secure channels for each CR-IoT transmission while satisfying a pre-specified QoS/throughput requirement and delay constraint. In addition to the fact that PCS-MAC is generic in the sense that it can be adopted by systems that use multi-carrier (i.e., multi-channel) transmission techniques or systems that are physi-

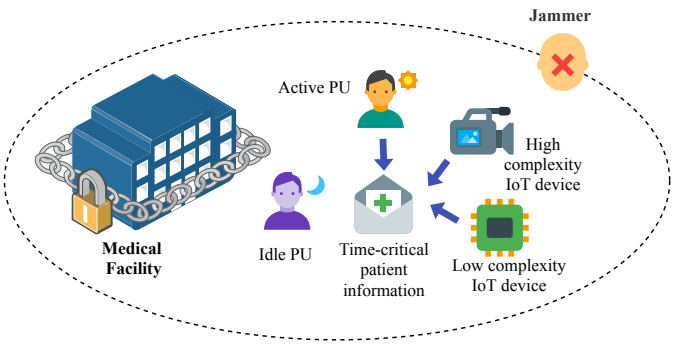


Fig. 1. CR-IoT-based network depicting the PUs and the SUs (IoT devices) trying to send time-critical patient information over the wireless channel and the jammer attempting to prevent their transmission.

cally equipped with multiple transceivers (i.e., multi-radio), two other contributions of work are summarized as follows:

- Mathematical modelling of the parallel-channel assignment problem that considers channel conditions, PUs activity, delay requirements, and throughput requirements while resisting jamming attacks without requiring additional nodes or hardware. Unlike the previously proposed techniques in literature for single-channel transmission, e.g., [23], our approach aims to provide multi-channel transmission for users to ripe multiplexing/diversity gains based on their application. Our derived solution turned out to be a non-linear binary problem (NLBP). To linearlize the NLBP problem, sequential-fixing linear programming (SFLP) procedure [26], [27] is used as a tool to solve the problem in polynomial time.
- Most of the work in literature is validated using simulations, yet simulators cannot fully mimic real-life implementation. Hence, to accurately analyze and validate the proposed algorithm, PCS-MAC, real-life experiments are used. The experiments are orchestrated to resemble practical deployment settings on a large-scale testbed, future Internet-of-things (FIT) IoT-LAB [28] and results are shown under various system conditions.

This work extends our previous work in [29]. Our current work considers two types of jamming attacks, namely proactive and reactive jamming; while [29] only considered proactive jamming threats. As a result, the optimization problem is reformulated. Additionally, this paper expands the analysis of the aforementioned work, by evaluating the performance of the proposed algorithm under various system design constraints, such as delay requirements and the number of available links for transmission.

C. Paper Structure

The rest of this paper is structured as follows: Section II details the network model, Section III depicts the PCS-MAC algorithm, and in Section IV, the chosen experimental testbed, FIT IoT-LAB, is introduced. Section V presents the results and finally the paper concludes in Section VI.

II. System Description and Jamming Analysis

Fig. 1 depicts the system model of this work, showing the different types of users who are sharing the wireless spectrum in the presence of jammers. Jammers main categories include constant, deceptive, proactive/random, and reactive [30]. The constant jammer corrupts all network packets by transmitting random signals continually. However, these types of attacks can be easily detected, as the source of the created interference can be traced [31]. A deceptive jammer sends constantly a stream of bytes similar to a legitimate transmission. The consistency of these attacks from a single source again makes them easily traceable. Furthermore, the two aforementioned attacks require a significant amount of power. Hence, in our analysis, we focused on the two latter types of attacks, the proactive and reactive jammers [12]. Proactive jammers alternate between sleeping and jamming phases without any regard to when CR nodes are transmitting. Reactive jammers, on the other hand, are the most energy-efficient type of attacks, as they start their transmissions only when CR transmission is detected. A thorough illustration of these two jamming strategies is provided in the forthcoming subsections. It is important to note that jammers can simply disregard MAC protocols and prevent legitimate users from using the network. Yet, the legitimate users have to abide by IEEE's MAC protocols, which are normally carrier sense multiple access/collision avoidance (CSMA/CA) based. Such attacks can also introduce packet collisions and force repeated backoffs [32].

A. Network Model

The CR-IoT-based network model consists of $\mathcal{M}$ channels and a set of links, $\mathcal{L}_x$, such that $\mathcal{M} \geq \mathcal{L}_x$. The number of links depends on the number of transceivers present in the CR-IoT nodes hardware architecture (in the case of multi-radio transmission) or the maximum number of channels assigned to this device (in the case of multi-channel transmission). It is important to note that in this analysis, we are considering a multi-channel environment as well as a multi-channel transmission capability of the devices. In this context, a communication link between any two CR-IoT devices can consist of one or multiple channels. Multi-channel transmission can be realized using frequency division multiplexing (FDM), discontiguous orthogonal frequency division multiplexing (D-OFDM) [33], or other multi-carrier schemes. Using a Markov renewal BUSY/IDLE alternating process, the status of each channel $i \in \mathcal{M}$ is modeled assuming all channels have equal bandwidths. $T_I^{(i)}$ denotes that the channel is available/idle, and thus it can be used by CR-IoT nodes. The duration $T_B^{(i)}$ denotes the time for which channel i is occupied by the PUs. Both durations can be modeled as Poisson random variables [23]. Assuming that PUs usage pattern slowly varies with time, CR-IoT devices can simply estimate PUs activity by conducting cooperative spectrum sensing [34]. As previously mentioned, we consider two types of jamming attacks, proactive and reactive jamming. In [12], a gambling-based model of proactive and reactive jammers in time-critical applications was developed and experimentally validated. The rationale behind the model was that a delay threshold can be set; a message would then become invalid if

this threshold was exceeded. Retransmissions of the message are seized if the transmission is successful, or if the delay threshold is surpassed. The analysis led to the development of the invalidity ratio metric, which encompassed the CSMA/CA protocol. The analysis in this work follows the same rationale presented in [12]. The behaviour of each type of attack and its impacts on the network performance are described below.

Proactive jammer: We consider a set of proactive jammers that attempt to corrupt the CR-IoT transmissions over the $\mathcal{M}$ available PU channels. The strategy of the proactive jammer attacking channel i, where $i = \{1, \cdots, \mathcal{M}\}$, can be described by the time interval between the successive jamming signals over channel i ($T_J^{(i)}$). For successful packet delivery, the packet transmission time, t_x, needs to be less than both the chosen CR channel idle period, $T_I^{(i)}$, in order not to interfere with PU activity, and the jamming interval across the channel, $T_J^{(i)}$, to ensure that the packet was not damaged by the jammer. For a given assignment $\Omega = \{m_1, m_2, \cdots, m_{\mathcal{M}}\}$, the failure probability, as defined in [23], can be expressed as:

$$\begin{aligned} p_p &= 1 - \Pr\Big(\{\min(T_I^{(i)}, T_J^{(i)})\} \geq t_x, \forall i \in \Omega\Big) \\ &= 1 - \prod_{i\in\Omega} \Pr\Big(\{\min(T_I^{(i)}, T_J^{(i)})\} \geq t_x\Big) \end{aligned} \tag{1}$$

Following the memoryless jamming model expressed in [35], where $T_I^{(i)}$ and $T_J^{(i)}$ are statistically independent and exponentially distributed random variables (with means of $\overline{T}_I^{(i)}$ and $\overline{T}_J^{(i)}$, respectively), then, p_p can be expressed as:

$$\begin{aligned} p_p &= 1 - \prod_{i\in\Omega} e^{-\frac{t_x}{\overline{T}_I^{(i)}}} e^{-\frac{t_x}{\overline{T}_J^{(i)}}} \\ &= 1 - \prod_{i\in\Omega} e^{-t_x \frac{\overline{T}_I^{(i)} + \overline{T}_J^{(i)}}{\overline{T}_I^{(i)} \overline{T}_J^{(i)}}} \\ &= 1 - \prod_{i\in\Omega} e^{-\lambda_i t_x}, \quad \lambda_i = \frac{\overline{T}_I^{(i)} + \overline{T}_J^{(i)}}{\overline{T}_I^{(i)} \overline{T}_J^{(i)}} \end{aligned} \tag{2}$$

Then, the failure probability after N_x MAC layer retransmission attempts is given by:

$$p_{f_p} = p_p^{N_x} = \Big(1 - \prod_{i\in\Omega} e^{-\lambda_i t_x}\Big)^{N_x} \tag{3}$$

Reactive jammer: For the case of reactive jamming, the condition for successful packet delivery occurs when the total transmission time of the CR-IoT packet is less than the idle period of the selected channel and no jamming to impact the packet occurs during that time. Since jamming and PU activities are independent random variables, the failure probability, p_r, as defined in [23], is evaluated as

$$\begin{aligned} p_r &= 1 - \prod_{i\in\Omega} \Pr(T_I^{(i)} > t_x)(1 - P_J^{(i)}) \\ &= 1 - \prod_{i\in\Omega} e^{-\frac{t_x}{\overline{T}_I^{(i)}}} (1 - P_J^{(i)}), \end{aligned} \tag{4}$$

where $P_J^{(i)}$ denotes the jamming probability over channel i. Similar to the case of proactive jamming, the failure probability after N_x retransmissions can be expressed as

$$p_{f_r} = p_r^{N_x} = \Big(1 - \prod_{i\in\Omega} e^{-\frac{t_x}{\overline{T}_I^{(i)}}} (1 - P_J^{(i)})\Big)^{N_x} \tag{5}$$

B. Invalidity Ratio Analysis

The packet-invalidity ratio, r, can be interpreted as the probability that the transmission delay of a data packet, D, exceeds a preset threshold, D_{th}. Invalidity ratio calculations take into account the jamming interval, the CR network link quality, and PU channel availability duration. A generalized upper bound for r (denoted as r^{up}), irrespective of the jammer type, can be calculated as [23]:

$$r \leq r^{up} = \frac{p_f \overline{d_k}}{(1 - p_f)(D_{th} - \overline{d_k}) + p_f \overline{d_k}}, \tag{6}$$

where $\overline{d_k}$ is the average MAC-layer delay of transmission k and p_f is failure probability after N_x re-transmissions. The aim is to select the channels that would enhance the CR network throughput for each transmission. In order to achieve this in the presence of a jammer, the algorithm must account for PU activity, link-quality, and jamming behaviour.

Given the upper bound r^{up}, a specific invalidity-rate requirement $r \leq \gamma$ can be ensured by imposing that $r^{up} \leq \gamma$, where the term γ presents the invalidity ratio threshold that is required to achieve predefined QoS requirements for IoT devices. This implies that $r \leq r^{up} \leq \gamma$, which ensures that $r \leq \gamma$. For a given γ, the upper bound in (6) can be equivalently written in terms of p_f as:

$$\begin{aligned} &\frac{p_f \overline{d_k}}{(1 - p_f)(D_{th} - \overline{d_k}) + p_f \overline{d_k}} \leq \gamma, \\ &p_f \overline{d_k} - \gamma(1 - p_f)(D_{th} - \overline{d_k}) - \gamma p_f \overline{d_k} \leq 0, \\ &p_f \big(\, \overline{d_k}(1 - 2\gamma) + \gamma D_{th} \,\big) \leq \gamma(D_{th} - \overline{d_k}), \\ &p_f \leq \frac{\gamma(D_{th} - \overline{d_k})}{(\, \overline{d_k}(1 - 2\gamma) + \gamma D_{th} \,)} = B_{th}^{(D_{th}, \gamma, \overline{d_k})}, \end{aligned} \tag{7}$$

where B_{th} is a threshold-dependant delay constant.

By using (3) into (7), the invalidity requirement can be written in terms of the failure probability, p, for a given assignment Ω as:

$$\begin{aligned} p^{N_x} &\leq B_{th}^{(D_{th}, \gamma, \overline{d_k})}, \\ p &\leq \sqrt[N_x]{B_{th}} \end{aligned} \tag{8}$$

Under proactive jamming, using (2) into (8) and some algebraic manipulation, the invalidity-ratio requirement for a given assignment Ω can be written as:

$$\begin{aligned} 1 - e^{-\sum_{i\in\Omega} \lambda^{(i)} t_x} &\leq \sqrt[N_x]{B_{th}}, \\ \ln\big(1 - \sqrt[N_x]{B_{th}}\big) &\leq -\sum_{i\in\Omega} \lambda^{(i)} t_x, \end{aligned} \tag{9}$$

where $t_x = L / \sum_{i\in\Omega} \mathcal{R}^{(i)}$ with L representing the packet size and and $\mathcal{R}^{(i)}$ is the rate of transmission in channel i.

Under reactive jamming scenarios, and for a given assignment Ω, the invalidity-rate requirement can be written in terms of the jamming behavior by applying (5) and (8) as:

$$\begin{aligned}
1-\prod_{i\in\Omega}\Pr(T_I^{(i)})(1-P_J^{(i)}) &\le \sqrt[N_x]{B_{th}}\\
(1-\sqrt[N_x]{B_{th}}) &\le \prod_{i\in\Omega} e^{-\frac{t_x}{\overline{T}_I^{(i)}}}(1-P_J^{(i)})\\
\ln(1-\sqrt[N_x]{B_{th}}) &\le \ln(\prod_{i\in\Omega} e^{-\frac{t_x}{\overline{T}_I^{(i)}}}(1-P_J^{(i)}))\\
\ln(1-\sqrt[N_x]{B_{th}}) &\le \sum_{i\in\Omega}\ln\left(e^{-\frac{t_x}{\overline{T}_I^{(i)}}}(1-P_J^{(i)})\right)\\
\ln(1-\sqrt[N_x]{B_{th}}) &\le \sum_{i\in\Omega}\left(\ln(1-P_J^{(i)})-\frac{t_x}{\overline{T}_I^{(i)}}\right)
\end{aligned} \tag{10}$$

III. Security-aware Multi-transceiver Channel Assignment Design with QoS Constraints

Our main objective is to enhance spectrum utilization by selecting the least number of secure channels for each CR-IoT transmission while satisfying pre-specified delay and QoS requirements in medical applications that carry time-critical information. By achieving this, IoT devices with various capabilities can coexist in the same network and the spectrum can be fairly shared. For each given CR-IoT-based transmission, the set of available channels with their average availability (and jamming) intervals, the received signal-to-noise ratio (SNR) over each channel, and the delay requirements are used to compute the most secure channel assignment (Ω) that satisfies the QoS requirements while using the minimum number of channels subject to the following network constraints:

1) **Physical constraint**: Each CR-IoT device is equipped with $\mathcal{L}_x$ transceivers or is assigned a maximum number of channels to occupy (based on the modulation technique), in other words, each CR user can utilize up to $\mathcal{L}_x$ channels at a time.
2) **The QoS constraints:** The invalidity ratio r, calculated using the specified delay requirements and jamming behaviour over the selected channels, must be less than a predefined threshold $r \le \gamma$. Mathematically, this constraint is given in (9). Additionally, the aggregate rate should be greater than a user-specified rate demand R_{th} based on the application requirements.
3) **The received SNR constraints:** The received SNR over each chosen channel $i \in \Omega$ must exceed a pre-specified threshold SNR_{th} (i.e., $\text{SNR}^{(i)} \ge \text{SNR}_{th}$).
4) **Exclusive-channel occupancy constraints:** Each idle channel cannot be assigned to more than one CR-IoT device at a time.

A. Problem Formulation

We have considered slowly-varying fading channels, in which the fading remains unchanged during the total transmission time of one packet. The appropriateness of this assumption has been demonstrated in [23], [25], [36] for CR-IoT operating environment. Recall that our channel assignment problem is investigated under proactive and reactive jamming attacks. In the analysis, perfect channel estimation (received SNR) is assumed, and hence the achieved rate over the different channels can be estimated. Given the achieved data rates over the different channels, the failure probability can be computed using (5). This section is dedicated to formulating the channel assignment problem under the two aforementioned types of attacks. To proceed in our analysis, a binary decision variable, $\alpha^{(i)}$, for each channel $i \in \mathcal{M}$ is defined as follows:

$$\alpha^{(i)} = \begin{cases} 1, & \text{if channel } i \text{ is chosen to be included in } \Omega \\ 0, & \text{otherwise.} \end{cases}$$

1) Problem Formulation under Proactive Jamming: Under proactive jamming, the invalidity constraint in (9) can be rewritten in terms of the decision variable $\alpha^{(i)}$ as follows:

$$\begin{aligned}
1-e^{-\sum_{i=1}^{|\mathcal{M}|}\lambda^{(i)}t_x\alpha^{(i)}} &\le \sqrt[N_x]{B_{th}}\\
\ln(1-\sqrt[N_x]{B_{th}}) &\le -\sum_{i=1}^{|\mathcal{M}|}\lambda^{(i)}t_x\alpha^{(i)}
\end{aligned} \tag{11}$$

Then, t_x can be re-expressed as $\frac{L}{\sum_{i=1}^{|\mathcal{M}|}\mathcal{R}^{(i)}\alpha^{(i)}}$.

By writing the design constraints in terms of $\alpha^{(i)}$, the multi-channel multi-transceiver security-aware channel assignment problem under proactive jamming can be formulated as:

$$\begin{aligned}
&\min_{\alpha_i\in\{0,1\}}\textstyle\sum_{i\in\mathcal{M}}\alpha^{(i)}\\
&\text{s.t.}\quad \textstyle\sum_{i=1}^{|\mathcal{M}|}\alpha^{(i)} \le \mathcal{L}_x\\
&\quad \ln(1-\sqrt[N_x]{B_{th}}) \le -\textstyle\sum_{i=1}^{|\mathcal{M}|}\lambda^{(i)}t_x\alpha^{(i)}\\
&\quad \textstyle\sum_{i=1}^{|\mathcal{M}|}\mathcal{R}^{(i)}\alpha^{(i)} \ge R_{th}\\
&\quad \text{SNR}^{(i)} - \text{SNR}_{th} \ge \Gamma(\alpha^{(i)}-1), \forall i \in \mathcal{M},
\end{aligned} \tag{12}$$

where Γ is a very large positive number. Note that the last constraint ensures that $\text{SNR}^{(i)} \ge \text{SNR}_{th}$ for any selected channel i (i.e., when the $\text{SNR}^{(i)} < \text{SNR}_{th}$, the left-hand-side of this constraint is a negative number, and hence the right-hand-side should be a very large negative number, and hence $\alpha^{(i)}$ should be 0. On the other hand if the $\text{SNR}^{(i)} \ge \text{SNR}_{th}$, then the left-hand-side is always ≥ 0, and hence $\alpha^{(i)}$ can be either 1 or 0 depending on the optimization problem).

Substituting $t_x = \frac{L}{\sum_{i=1}^{|\mathcal{M}|}\mathcal{R}^{(i)}\alpha^{(i)}}$ into (11) and using some algebraic manipulation, the second constraint of (12) can be rewritten in a linear form as:

$$\sum_{i\in\mathcal{M}}\left(\mathcal{R}^{(i)}\ln(1-\sqrt[N_x]{B_{th}})+L\lambda^{(i)}\right)\alpha^{(i)} \le 0 \tag{13}$$

By letting $\mathcal{R}^{(i)}\ln(1-\sqrt[N_x]{B_{th}})+L\lambda^{(i)} = a_i$, the second constraint in (12) becomes $\sum_{i=1}^{|\mathcal{M}|}a_i\alpha^{(i)} \le 0$. It is important to note that the constant a_i does not have a physical meaning, it is only defined to simplify our analysis and write the invalidity constraint in a more compact manner. The last constraint can be simply guaranteed by setting $\alpha^{(i)} = 0,\ \forall i$ with

$\text{SNR}^{(i)} < \text{SNR}_{th}$. Therefore, the optimization problem in (12) becomes:

$$\begin{aligned} \min_{\alpha_i \in \{0,1\}} & \sum_{i \in \mathcal{M}} \alpha^{(i)} \\ \text{s.t.} \quad & \sum_{i=1}^{|\mathcal{M}|} \alpha^{(i)} \leq \mathcal{L}_x \\ & \sum_{i=1}^{|\mathcal{M}|} a_i \alpha^{(i)} \leq 0 \\ & \sum_{i=1}^{|\mathcal{M}|} \mathcal{R}^{(i)} \alpha^{(i)} \geq R_{th} \end{aligned} \tag{14}$$

2) Problem Formulation under Reactive Jamming: Under reactive attacks and after the mathematical steps provided at the top of the next page, the invalidity constraint can be written in terms of $\alpha^{(i)}$ as:

$$\sum_{i=1}^{\mathcal{M}} b_i \alpha^{(i)} \leq \sum_{j=1}^{\mathcal{M}} \sum_{i=1}^{\mathcal{M}} c_{ij} \alpha^{(i)} \alpha^{(j)}, \tag{16}$$

where $b_i = \ln(1 - \sqrt[N_x]{B_{th}})\mathcal{R}^{(i)} + L$ and $c_{ij} = \ln(1 - P_J^{(i)})\ \mathcal{R}^{(j)}$. Note that the optimization problem is the same as in the case of the proactive jammer but with (16) replacing the 2nd constraint. Up to this point, the formulation is an NLBP problem. In an attempt to linearize the problem, the non-linear constraint in (16) can be written in a linear form by replacing the quadratic term $\alpha^{(i)}\alpha^{(j)}$ with $w_{ij}\ \forall i,\ j \in \mathcal{M}$ (i.e., $w_{ij} = \alpha^{(i)}\alpha^{(j)}$) and introducing the following linear set constraints on w_{ij}:

$$\begin{aligned} & w_{ij} \leq \alpha^{(i)} \\ & w_{ij} \leq \alpha^{(j)} \\ & w_{ij} \leq \alpha^{(i)} + \alpha^{(j)} - 1 \end{aligned} \tag{17}$$

Note that if either $\alpha^{(i)}$ or $\alpha^{(j)} = 0$, then $w_{ij} = 0$ and if both $\alpha^{(i)}$ or $\alpha^{(j)} = 1$, then, $w_{ij} = 1$. Thus, it is an exact formulation. This will yield $3 \times \mathcal{M} \times \mathcal{M}$ constraints to the problem formulation. Thus, the constraint in (16) becomes:

$$\begin{aligned} & \textstyle\sum_{i=1}^{\mathcal{M}} b_i \alpha^{(i)} - \sum_{j=1}^{\mathcal{M}} \sum_{i=1}^{\mathcal{M}} c_{ij} w_{ij} \leq 0 \\ & w_{ij} \leq \alpha^{(i)} && \forall i \in \mathcal{M}, j \in \mathcal{M} \\ & w_{ij} \leq \alpha^{(j)} && \forall i \in \mathcal{M}, j \in \mathcal{M} \\ & w_{ij} \leq \alpha^{(i)} + \alpha^{(j)} - 1 && \forall i \in \mathcal{M}, j \in \mathcal{M} \end{aligned} \tag{18}$$

Now, we have $\mathcal{M}$ $\alpha^{(i)}$ variables and $\mathcal{M}^2$ w_{ij} variables. By replacing the non-linear constraint with its equivalent linear form given in (18), the problem formulation under reactive jamming becomes:

$$\begin{aligned} \min_{\alpha_i \in \{0,1\}} & \textstyle\sum_{i \in \mathcal{M}} \alpha^{(i)} \\ \text{s.t.} \quad & \textstyle\sum_{i=1}^{|\mathcal{M}|} \alpha^{(i)} \leq \mathcal{L}_x \\ & \textstyle\sum_{i=1}^{\mathcal{M}} b_i \alpha^{(i)} - \sum_{j=1}^{\mathcal{M}} \sum_{i=1}^{\mathcal{M}} c_{ij} w_{ij} \leq 0 \\ & \textstyle\sum_{i=1}^{|\mathcal{M}|} \mathcal{R}^{(i)} \alpha^{(i)} \geq R_{th} \\ & w_{ij} \leq \alpha^{(i)} && \forall i \in \mathcal{M}, j \in \mathcal{M} \\ & w_{ij} \leq \alpha^{(j)} && \forall i \in \mathcal{M}, j \in \mathcal{M} \\ & w_{ij} \geq \alpha^{(i)} + \alpha^{(j)} - 1 && \forall i \in \mathcal{M}, j \in \mathcal{M} \end{aligned} \tag{19}$$

As a result, there will be $3 + 3 \times \mathcal{M}^2$ constraints.

B. The Proposed Solution

The problem formulations in (14) and (19) can be observed as a binary linear programming (BLP) optimization problems. Generally, the optimal solution to these problems is NP-hard. To solve this problem in polynomial-time, the SFLP procedure [26], [27] is used as a tool to find a near-optimal solution for our BLP problem. The effectiveness of the SFLP procedure in solving BLP problems have been demonstrated in several previous works, where near-optimal solutions were provided in polynomial-time [21]–[23], [26], [27]. Thus, our problem in (14) can be near-optimally solved in polynomial-time using the SFLP procedure. The proposed channel assignment algorithm operates as follows:

1) Given SNR_{th}, the channels that do not satisfy the SNR threshold will be excluded from $\mathcal{M}$, yielding a new set of feasible channels $\mathcal{M}^f$. Then, the algorithm arbitrates the per-channel achievable rate, $\mathcal{R}^{(i)}$, and the required per-channel transmission period accordingly, i.e., $t_x^{(i)} = L/\mathcal{R}^{(i)}$.
2) Using $T_I^{(i)}, T_J^{(i)}, B_{th}, N_x,$ and $\mathcal{R}^{(i)}$, the algorithm calculates the jammer type dependent variable, $a^{(i)}$ in the case of the proactive jamming and b_i and c_{ij} for reactive jamming, for the renewed set obtained from step 1.
3) The findings are fed to the SFLP procedure and $\alpha^{(i)}$'s are computed.
4) If the SFLP fails to find a solution, i.e., a solution such that the throughput constraint is satisfied cannot be found, the algorithms chooses $\mathcal{L}_x$ channels with the highest invalidity ratios. In this case, we donate the binary decision variation as $\alpha^{*(i)}$.

Algorithm 1 shows the pseudocode of PCS-MAC. In our analysis, we have consider a single-hop distributed ad-hoc CR-IoT network, where each CR user can directly communicate with any other CR user. In such types of networks, there is no access point (AP) to coordinate the transmissions and allocate channels to each node. In a single-hop single collision domain, where all nodes can hear each other, all control information exchanges can be heard by all CR-IoT devices. This ensures that all contending CR-IoT devices will have the same updated channel occupancy and channel avoidance information. Due to the absence of an AP, our solution includes developing a distributed channel access mechanism that allocates channels to CR-IoT devices using a CSMA/CA-based mechanism implemented over a common control channel. Using a handshaking procedure, CR-IoT to CR-IoT inference can be eliminated. However, with that being said, our solution can be easily adopted in a centralized CRN with an AP, which significantly simplifies the spectrum access protocol as the CR-IoT users can only communicate with the AP.

The proposed algorithm is efficient in consuming resources overall. The algorithm uses carrier sensing and calculations based on locally estimated metrics such as signal-to-noise ratio and packet delivery ratio along with available information about PU activities, which is available to all algorithms in CR-based networks. Our algorithm does not require the nodes to exchange any non-user data information for the sake of detecting and mitigating the jamming attack. In general, anti-

$$
\begin{aligned}
\ln(1-\sqrt[N_x]{B_{th}}) &\leq \sum_{i=1}^{\mathcal{M}} \Big(\ln(1-P_J^{(i)})\ \alpha^{(i)} - \frac{t_x}{\overline{T}_I^{(i)}}\alpha^{(i)} \Big) \\
&\leq \sum_{i=1}^{\mathcal{M}} \Big(\ln(1-P_J^{(i)})\ \alpha^{(i)} - \frac{L\ \alpha^{(i)}}{\overline{T}_I^{(i)} \sum_{j=1}^{\mathcal{M}} \mathcal{R}^{(j)}\alpha^{(j)}} \Big) \\
\sum_{i=1}^{\mathcal{M}} \Big(\ln(1-\sqrt[N_x]{B_{th}})\overline{T}_I^{(i)}\mathcal{R}^{(i)} \Big)\alpha^{(i)} &\leq \sum_{j=1}^{\mathcal{M}}\sum_{i=1}^{\mathcal{M}} \Big(\ln(1-P_J^{(i)})\ \overline{T}_I^{(i)}\ \mathcal{R}^{(j)}\alpha^{(i)}\alpha^{(j)} - L\ \alpha^{(i)} \Big) \\
\sum_{i=1}^{\mathcal{M}} \Big(\ln(1-\sqrt[N_x]{B_{th}})\ \overline{T}_I^{(i)}\mathcal{R}^{(i)} + L \Big)\alpha^{(i)} &\leq \sum_{j=1}^{\mathcal{M}}\sum_{i=1}^{\mathcal{M}} \ln(1-P_J^{(i)})\ \overline{T}_I^{(i)}\ \mathcal{R}^{(j)}\alpha^{(i)}\alpha^{(j)}
\end{aligned}
\tag{15}
$$

Algorithm 1 PCS-MAC channel assignment

Input: $\mathcal{M}$, B_{th}, N_x, $\mathcal{L}_x$, SNR_{th}, $\text{SNR}^{(i)}$, $T_I^{(i)}$, $T_J^{(i)}$, $\mathcal{R}^{(i)}$
Output: A feasible multi-channel assignment is found and given by $\alpha^{(i)}$ or no feasible assignment can be found
Let $\mathcal{M}^f = \mathcal{M}$
for all $i \in \mathcal{M}$
  if $\text{SNR}^{(i)} <\ \text{SNR}_{th}$
    $\mathcal{M}^f = \mathcal{M}^f - \{i\}$
  else Compute the invalidity ratio $r^{(i)}$
    Compute a_i or b_i and c_{ij} based on the jammer strategy
  end-of-if
end-of-for
$\alpha^{(i)}$ = SFLP
if $\alpha^{(i)} = \phi$
  for all $i \in \mathcal{M}_j^f$
    Sort the channels in an increasing order of $r^{(i)}$
  end-of-for
  Let $\mathcal{U}$ be the sorted channel list
  Identify the $\mathcal{L}_x$ channels that are on the top of $\mathcal{U}$
  Return $\alpha^{*(i)}$
else Return $\alpha^{(i)}$
end-of-if

jamming techniques in WSNs and IoT networks require more resources to accomplish the detection and mitigation of the jamming attack. JAM protocol [37] detects the presence of jamming based on lost messages and mitigates that by mapping the jammed area and avoid sending through that area. The mapping process involves sending additional messages that consume bandwidth and power resources of the communicating nodes. In addition, such protocols assume high redundancy in routers/switches and links to be able to produce a redundant path. Ant system [38] employs agents that travel the networks periodically to detect the presence of compromised nodes and/or jammed links to avoid communicating through these links. Agents' messages represent an overhead with respect to bandwidth resources. The hybrid anti-jamming system [39] is based on replicating based stations to allow establishing multiple paths among them in case jamming attack. This solution requires additional equipment resources.

It is important to note that based on the findings in [12], there exists a phase transition phenomenon of packet delivery performance. For reactive jamming, it was observed that when jamming probability, $P_J^{(i)}$, increases, the packet invalidity ratio ($r^{(i)}$) first increases slightly, then increases dramatically to 1. For non-reactive (proactive) jamming, there exists a similar phenomenon. When the average jamming interval, $T_J^{(i)}$, increases, the message invalidity ratio first has the value of 1, then decreases dramatically to 0. In this paper, the same rationale is used to adjust the anti-jamming algorithm by identifying the type of attack based on the variation of the value of $r^{(i)}$. Initially, the jamming attack is assumed to be proactive. Then, with every transmission, the invalidity ratio is re-calculated and its value is compared to the previous transmission to determine if the strategy needs to be reversed.

C. Complexity Analysis

The MAX-PoS algorithm presented in [21], [22] was proven to have a polynomial-time complexity that is bounded by the linear programming (LP) solver's complexity times the number of PU channels, $\mathcal{M}$. Our proposed channel assignment algorithm is proven to have a comparable worst-case time complexity to that of the reference MAX-PoS algorithm.

Theory: The proposed SFLP channel assignment algorithm's worst-case time complexity is polynomial in the number of PU channels ($2 \times \mathcal{M}$), which is determined by $\mathcal{M}$ iterations.

Proof: The proposed method guarantees that one new variable is fixed to either 0 or 1 in each iteration, and a new viable relaxed LP (RLP) issue is generated for the following iteration. A maximum of L_x iterations are required if all generated RLPs are feasible. If not, a maximum of $2 \times \mathcal{M}$ iterations are required to evaluate whether a feasible channel assignment can be determined. The worst-case scenario can be simulated by fixing all $\alpha^{(i)}$ variables to 0, which indicates that no feasible secure channel assignment can be found). As a result, the time complexity of our SFLP is limited by the LP solver's complexity times $\mathcal{M}$. The complexity of our proposed channel assignment algorithm is polynomial because the LP solver has a polynomial-time complexity. Therefore, the proposed channel assignment algorithm has a comparable

worst-case time complexity to that of the reference MAX-PoS algorithm. This is because both algorithms are based on an SFLP procedure with polynomial-time complexity.

IV. Experimental Testbed

A. Motivation

To analyze novel IoT protocols and algorithms, researchers resort to various methods [40]. Theoretical analysis brings the first proof-of-concept and aids in evolving a prediction of the system's characteristics and behavior. However, for accurate predictions, highly detailed models must be used which are frequently complex and difficult to comprehend and handle [41]. Simulators are the most adopted methods for system development and verification [42], as they yield a more realistic evaluation of the system's performance in comparison to pure theoretical evaluations. Additionally, testing and debugging is allowed on protocols at any design stage. Nevertheless, the reliability of simulators naturally depends on the accuracy of the used models, e.g., channel and energy consumption models, thus the results may not match real world experimentation. Additionally, most simulators do not consider the hardware limitations of the utilized nodes which normally have cogent impacts on the accuracy of the reported results. As a result, a hybrid method that merges hardware and software components for experimentation, the emulator, is introduced. Yet, emulators suffer from a high cost per tested node, limited scalability, low speed, and are platform dependent [42].

The stringiest approach is composing real world experiments. Unfortunately, they come at the expense of high software and hardware cost, plus the required manpower for installment and maintenance [40]. Testbeds, contrarily, provide realistic assessment, under factual channel conditions, without the entailed disadvantages of real world experimentation. Recently, a number of facilities started providing experimental testbeds that offer a magnitude of tools and services for researchers and developers [43]. After exhaustive search and evaluation, FIT IoT-LAB testbed is found to be the most apt for evaluating our CR-IoT-based implementation.

B. FIT IoT-LAB

FIT IoT-LAB is a member of the OneLab consortium. It has six different locations spread across France [28]. In total, it is made up of more than 2700 low-power wireless IoT sensor nodes and over one hundred mobile robots equipped with low-rate wireless personal area network (LR WPAN) connectivity, i.e., IEEE 802.15.4 standard. The testbed offers an environment that is multi-user, open-source, and open-access for experimentation. Node reservation and firmware deployment can either be made via a web-based portal or through command-line tools. The static nodes are divided into three types; WSN430, M3, and A8. The M3 nodes are chosen in our implementation. The nodes are equipped with a set of sensors and a radio interface via the AT86RF231 radio chip, which is IEEE 802.15.4 complaint. They are based on a 32-bit ARM Cortex-M3 micro-controller and operated by 3.7V lithium polymer (LiPo) battery. The IEEE 802.15.4 standard mandates both the physical and MAC layers; stating a communication range of 10–100 m using 16 orthogonal frequencies around 2.4 GHz, i.e., channels 11–26 [44]. Moreover, the standard specifies a maximum frame size of 127 bytes. On the software side, the M3 nodes can be managed via RIOT, OpenWSN, FreeRTOS, and Contiki. FreeRTOS is used, in this work, as it provides fast execution, small memory footprint, and low overhead. It is a micro-kernel that provides semaphores, mutexes, multi-threading, and software timers with a CSMA/CA for the MAC layer implementation.

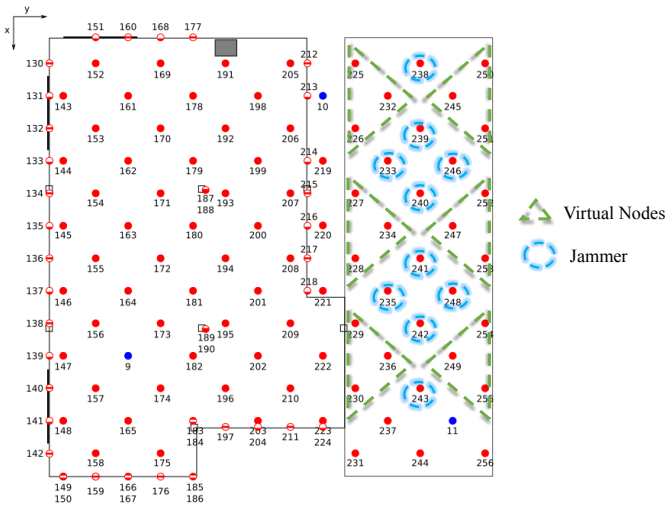
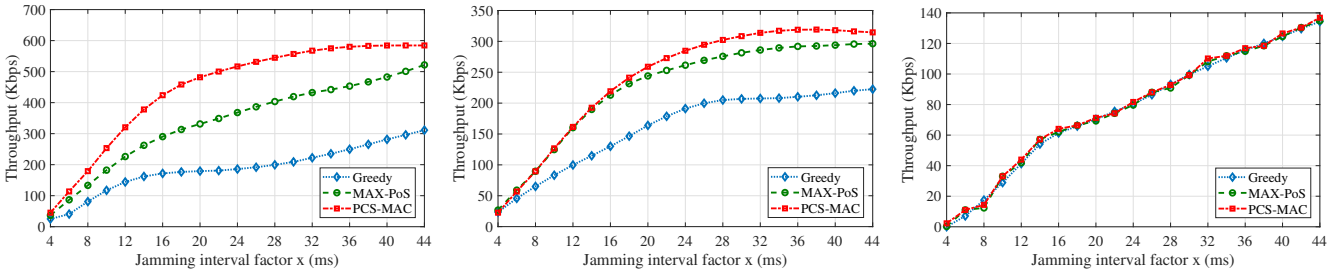


Fig. 2. The dedicated room used in our implementation located on the third floor of the building, depicting the M3 nodes mounted on the ceiling as solid red dots. They are placed in the form of a grid with a vertical and horizontal separation distance of 0.6m between each two consecutive nodes [45].

The Lille testbed, one of the six FiT IoT-LAB testbeds, is chosen for our experiments. It is deployed over three floors of a commercial building, through offices, corridors and a dedicated room with an area of $225\ \mathrm{m}^2$. Nodes in the room are spread over ceilings and wood poles, in our implementation we utilize the ceiling mounted nodes. These nodes are arranged in staggered rows over a $1.2\ \mathrm{m} \times 1.2\ \mathrm{m}$ grid at a height of $9.6\ \mathrm{m}$ from the floor. In total, the Lille site consists of 256 fixed and 3 mobile M3 nodes. This specific site is chosen as it provides great similarity to the targeted medical IoT environment with its high density of IoT nodes and the expected competition over the spectrum. Fig. 2 depicts the topology of the Lille site with the red dots denoting the M3 nodes, while the blue ones are Zolertia Firefly nodes. An experiment starts with the user communicating with the testbed via the web portal or the representational state transfer (REST) application program interface (API) through a secure shell (ssh) access and command line interface (CLI). The user can edit the source code, build/deploy firmware, and remotely debug the nodes.

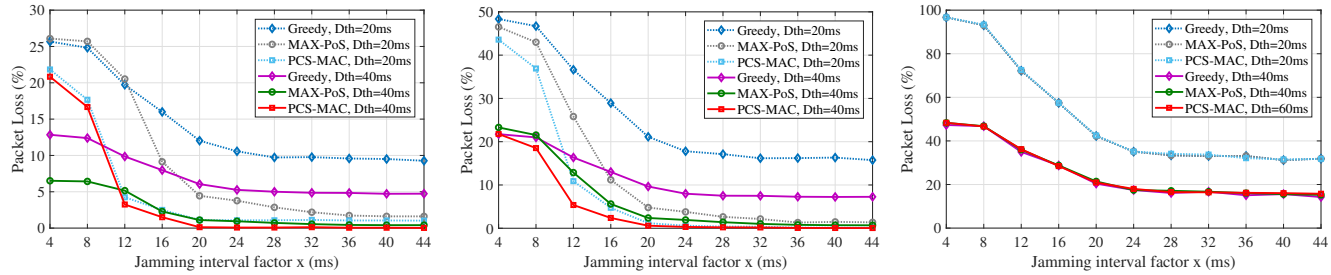
V. Results

In our implementation, performance is measured with throughput as the main metric. To administer the implementation, we generated custom firmwares based on the libraries supplied by the manufacturer of the nodes, HiKoB. We created two firmwares, one for the nodes acting as CR devices and



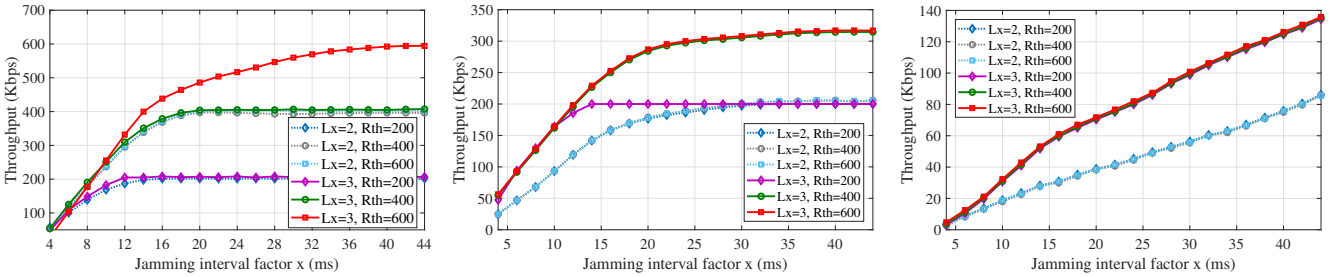
(a) Low PU activity with $P_B = 0.1$ (b) Moderate PU activity with $P_B = 0.5$ (c) High PU activity with $P_B = 0.9$

Fig. 3. Throughput curves of the proposed PCS-MAC channel assignment algorithm *vs.* the greedy and MAX-PoS algorithms for various busy probabilities, P_B, at $\mathcal{M} = 10$ and $L = 96$ bytes under proactive jamming and $\mathcal{L}_x = 3$.



(a) Low PU activity (b) Moderate PU activity (c) High PU activity

Fig. 4. Percentage of dropped packets of the proposed PCS-MAC channel assignment algorithm *vs.* the greedy and MAX-PoS algorithms for different delay requirements, D_{th}, under proactive jamming and $\mathcal{L}_x = 3$.

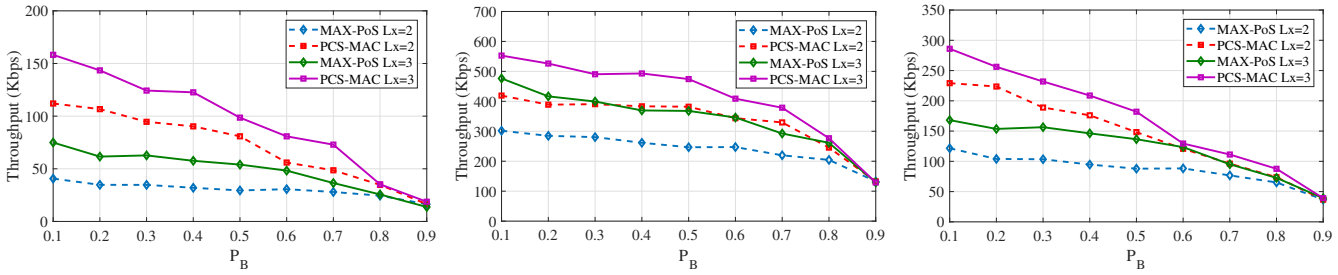


(a) Low PU activity (b) Moderate PU activity (c) High PU activity

Fig. 5. Throughput curves of the proposed PCS-MAC channel assignment algorithm under proactive jamming at $\mathcal{L}_x = 2$ and $\mathcal{L}_x = 3$ for various QoS requirements.

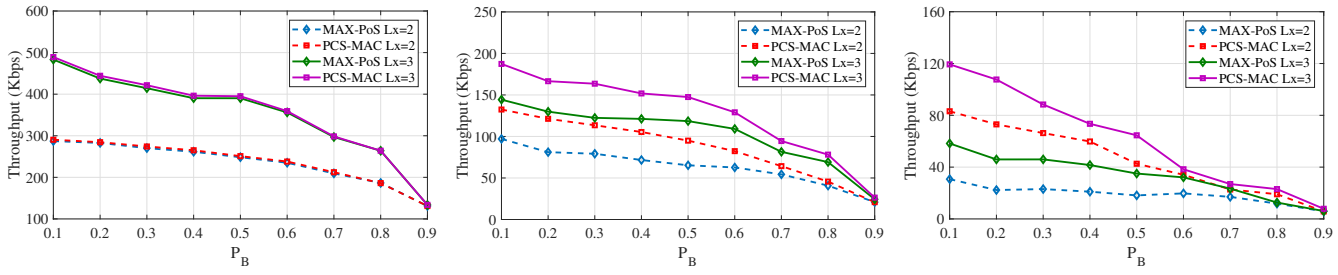
another for the nodes acting as jammers. The CR devices firmware adopts the FreeRTOS-based CSMA/CA MAC and performs channel condition assessment at the beginning of each transmission. Then, based on the gathered information and user set parameters (e.g., delay and throughput requirements), the algorithm is performed on the nodes and the channels are selected. The nodes try to send their packets over the assigned channels, and are allowed to retransmit the packets (in case the packets were damaged by the jammer) as long as the delay threshold is not exceeded. On the other hand, the jammers are programmed to constantly send out packets at fixed intervals, based on the parameter x in the proactive jammer case and p_J^{MAX} for reactive jammers. Throughput performance is investigated using two reference algorithms: MAX-PoS [21], [22] and the greedy approach. The MAX-PoS algorithm, as mentioned in the related work section, is a probabilistic-based approach that aims at maximizing network throughput by utilizing the parallel-transmission capability while considering channel quality and availability. However, it is oblivious to jamming. On the other hand, the greedy algorithm aims at selecting the channels with the highest quality in terms of signal-to-noise ratio [46]. Due to the controlled nature of the testbed and the adopted standard, which is the LR-WPAN in FIT IoT-LAB as discussed in Section V, the transmission power and range are limited. Hence, the variations among the channels are minimal, causing the greedy algorithm to behave as a random channel selection algorithm.

In our experiment, there are 10 nodes reserved to act as jammers on the selected channels, which are channels 11 to 21. The positions of the jammers are fixed, however, the channels they jam vary with each run, such that all ten channels are jammed in every iteration. Channel 17, where FIT IoT WiFi access points operate, is excluded to



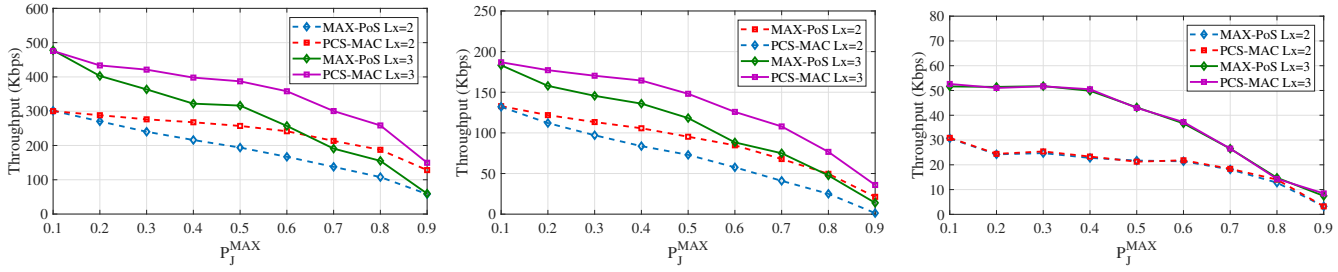
(a) High jamming activity (b) Moderate jamming activity (c) Low jamming activity

Fig. 6. Throughput performance vs. P_B under different jamming activities at $\mathcal{M} = 10$ and $L = 96$ bytes under proactive jamming at $\mathcal{L}_x = 2$ and $\mathcal{L}_x = 3$, i.e., given two and three transceivers.



(a) Low p_J^{MAX} (b) Moderate p_J^{MAX} (c) High p_J^{MAX}

Fig. 7. MAX-PoS and PCS-MAC throughput performance vs. P_B under different jamming activities at $\mathcal{M} = 10$ and $L = 96$ bytes for reactive jamming at $Lx = 2$ and $Lx = 3$, i.e., given two and three transceivers.



(a) $P_B = 0.1$ (b) $P_B = 0.5$ (c) $P_B = 0.9$

Fig. 8. Throughput performance vs. P_J^{MAX} under three primary user blocking probabilities at $\mathcal{M} = 10$ and $L = 96$ bytes under reactive jamming at $\mathcal{L}_x = 2$ and $\mathcal{L}_x = 3$, i.e., given two and three transceivers.

avoid external interference. Since single-radio multi-channel implementations introduce channel switching delays [47], in this paper, PCS-MAC is evaluated for the multi-radio case to allow fair evaluation of the proposed scheme. Since the M3 nodes have only one transceiver, virtual nodes are created by combing $\mathcal{L}_x$ physical M3 nodes to emulate CR-IoT nodes with parallel transmission capability. Fig. 2 shows how the virtual nodes are created by combining $\mathcal{L}_x$ M3 nodes to form nodes with parallel channel transmission capabilities, with a special example of $\mathcal{L}_x = 3$. There are six reserved virtual nodes, equivalent to 18 M3 nodes in the case of $\mathcal{L}_x = 3$ and 12 in the case of $\mathcal{L}_x = 2$. Each CR transmission occurs between two randomly selected virtual nodes and is fixed as 1000 packets, each is 96 bytes in length, i.e., $L = 96$ bytes. As previously mentioned in Section IV, the radio chip embedded on the nodes is built to be compliant with IEEE 802.15.4, with a maximum throughput of 250 Kbps. On top of the radio interface, the nodes are rigged with various sensors like; light, pressure, accelerometer, and gyrometer, that have to be initialized at the beginning of each run. Hence, the throughput is affected by the processing overhead in software, limiting the throughput far below the hardware maximum attainable rate. It was observed that the throughput of a single link fairly exceeds 200 Kbps, even in the absence of a jammer. Moreover, the transmission power is set to 1 dBm, following the testbed regulations which specifies a maximum transmission power of 5 dBm. Since the nodes' radio chip measures radio signal strength indicator (RSSI) by design [48], for simplicity of implementation, the RSSI is used instead of the SNR as the link-quality measure, setting a threshold of -70 dBm as our μ. Considering a time-critical application, a delay threshold of 20 ms is set, i.e., $D_{th} = 20$ ms [12]. Additionally, the maximum number of MAC layer retransmissions and the average MAC-layer delay $\overline{d_k}$ are respectively fixed to $N_x = 2$

and 1 ms. These values have been demonstrated in [12], [23], [49] to be applicable in a realistic wireless IoT scenarios.

A. Proactive Jammer

As previously mentioned, a memoryless jamming strategy is considered to emulate the proactive jamming attacks. The average availability duration, $T_I^{(i)}$, over the ten channels is 5, 100, 30, 5, 45, 50, 100, 5, 45, and 30 ms, respectively. While, the average jamming interval, $T_J^{(i)}$, over the ten channels is 5, 0.2, 10, 2, 20, 5, 0.1, 2.9, 20, and $0.2 \times x$ ms, respectively, where x represents the jamming attack level. Each channel is busy with probability P_B. Firstly, the throughput performance under different PU activity levels is investigated and presented in Fig. 3 for $\mathcal{L}_x = 3$ and $R_{th} = 600$ Kbps, as it is about the highest achievable throughput given 3 transceivers. The reported results are averaged over 1000 runs with the number of allowed MAC re-transmissions fixed as 2 ($N_x = 2$). In Fig. 3(a), $P_B = 0.1$ denotes that the 9 channels out of the available 10 can be occupied by CR transmission. As shown, the proposed technique outperforms the greedy approach significantly, yielding about 180% increase in throughput at $x = 20$ ms. PCS-MAC also outperforms MAX-PoS, with a 62% increase in throughput at $x = 20$ ms and $P_B = 0.1$. As x increases, the jamming attacks become less severe, which is intuitive as the period between jamming attacks becomes larger. Throughput, in return, increases with x. However, as x increases, PUs activities become the dominant obstacle for throughput performance. For high values of x, it can be observed that the performance of MAX-PoS approaches that of PCS-MAC, as the effect of jamming is reduced. Moreover, as the busy probability increases to reach 0.9, i.e., there is only one available channel to use, the limiting factor becomes channel availability. Thus, the performance of all algorithms is similar due to the lack of idle channels, shown in Fig. 3(c).

To evaluate the efficacy of the proposed algorithm in adapting to various delay requirements, Fig. 4 shows the effect of varying the delay threshold on the percentage of dropped packets. Intuitively, the larger the D_{th} the more time is allowed for packets to be retransmitted, hence, the number of dropped packets decreases. In Fig. 4(a), under low PU activity (i.e., $P_B = 0.1$), it can be observed that PCS-MAC outperforms the other techniques by having the least percentage of dropped packets in both delay requirements. However, similar to the previous results, at high PU activity (i.e., $P_B = 0.9$) all techniques behave similarly ascribed to the lack of available channels. Due to the lack of space and since the performance of PCS-MAC significantly outperforms that of the greedy approach, the remainder of the results focus on comparing PCS-MAC with MAC-PoS. The efficiency of PCS-MAC is also tested for different R_{th} requirements. Fig. 5 shows the throughput performance at three different data-rate requirements under different PU activity levels at $\mathcal{L}_x = 2$ and 3. As can be observed, the algorithm conforms to the specified requirement. In Fig. 5(c), since the throughput is already below the required R_{th}, the performance is identical to PCS-MAC in Fig. 3(c) at $\mathcal{L}_x = 3$. Lastly, the effect of varying P_B on the throughput is investigated in Fig. 6 for the cases of the nodes equipped with 2 and 3 transceivers. Throughput naturally increases as the number of transceivers increases for MAX-PoS and PCS-MAC. The resilience of PCS-MAC against jamming is highlighted in Fig. 6. For high jamming activity, the variance between the throughput performance of PCS-MAC and MAX-PoS is at its peak, as PCS-MAC reduces the number of dropped (invalid) packets which in return increases throughput. As the jamming level decreases, the variance between the throughput enhancement of both techniques declines, yet PCS-MAC is consistently to the fore.

B. Reactive Jammer

This section is dedicated to evaluating PCS-MAC under reactive jamming strategy. In this case, the jamming strategy is varied such that each channel i has a jamming probability $p_J^{(i)}$. For the ten channels, the jamming probabilities are 0.06, 0.75, 0.03, 0.15, 0.015, 0.06, 1, 0.105, 0.015, and $0.75 \times p_J^{MAX}$. The jamming probability factor, p_J^{MAX}, is bounded such that $0 \leq p_J^{MAX} \leq 1$ forcing the jamming probability of all channels not to exceed 1, which allows us to study throughput performance under different jamming conditions. Firstly, throughput is investigated under low, moderate, and high jamming activities vs. P_B, depicted in Fig. 7. Similar to the case of proactive jamming, the effectiveness of PCS-MAC prevails as the jamming attacks are more severe, i.e., high p_J^{MAX}. The throughput improvement is smaller at lower jamming probabilities, as the dominating factors are the channel quality and PUs activities, which are already addressed by MAX-PoS. However, at high p_J^{MAX} and $P_B = 0.1$, about a 100% throughput enhancement over MAX-PoS can be achieved by PCS-MAC using 2 or 3 transceivers, as depicted in Fig. 7(c). Fig. 8 studies the outcome of varying PU activities on throughput *vs.* p_J^{MAX}. It can be noticed that as $P_B = 0.9$, the performance of PCS-MAC gracefully degrades to that of MAX-PoS due to the lack of available idle channels. It can also be observed that throughput is inversely proportional to p_J^{MAX}, surrendering to its worst value at $p_J^{MAX} = 0.9$, as the jamming attacks become most vigorous. It is important to highlight that the network throughput correlates to the number of served users. Hence, the number of users N depends heavily on the number of available idle channels for CR-IoT devices to utilize, which depends on the PU activity level.

VI. Conclusion

In this paper, PCS-MAC was presented as a novel multi-channel assignment algorithm for delay-sensitive QoS constrained IoT-based CR networks under jamming attacks. Our algorithm assigned the least number of channels required for pre-set QoS and delay requirements while taking into account jamming activities, channel availability, and channel quality conditions. Using a probabilistic-based approach, the proposed algorithm counter-measured jamming attacks without requiring additional hardware, such as dedicated nodes or sensors. PCS-MAC performance was experimentally compared

with the MAX-PoS and greedy algorithms using the FIT-IoT testbed. The proposed algorithm was tested under various conditions: PU activity levels, delay requirements, throughput requirements and jamming attack levels. Results showed that a significant throughput improvement can be achieved in comparison to the other channel assignment algorithms.

REFERENCES

[1] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of things build our future: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2011–2027, 2018.

[2] J. Lin, *et al.*, "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[3] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 2015.

[4] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of things in the age of machine learning and software-defined networking," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4829–4829, Dec. 2018.

[5] Z. Wei and B. Hu, "A fair multi-channel assignment algorithm with practical implementation in distributed cognitive radio networks," *IEEE Access*, vol. 6, pp. 14255–14267, Feb. 2018.

[6] H. Bany Salameh, H. Al-Obiedollah, R. Mahasees, and Y. Jararweh, "Opportunistic non-contiguous OFDMA scheduling framework for future B5G/6G cellular networks," *Simul. Model. Prac. Theory*, vol. 119, Sep. 2022.

[7] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2015.

[8] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2011.

[9] S. Bhunia, E. Miles, S. Sengupta, and F. Vázquez-Abad, "CR-Honeynet: A cognitive radio learning and decoy-based sustenance mechanism to avoid intelligent jammer," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 3, pp. 567–581, Sep. 2018.

[10] L. Almon, M. Riecker, and M. Hollick, "Lightweight detection of denial-of-service attacks on wireless sensor networks revisited," in *Proc. IEEE LCN,* 2017.

[11] X. Wang, *et al.*, "Dynamic spectrum anti-jamming communications: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 79–85, Feb. 2020.

[12] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1746–1759, Aug. 2014.

[13] T. Amin, D. B. Rawat, and M. Song, "Performance analysis of secondary users in the presence of attackers in cognitive radio networks," in *Proc. IEEE GLOBECOM,* 2015.

[14] D. B. Rawat, O. Malomo, C. Bajracharya, and M. Song, "Evaluating physical-layer security for secondary users in cognitive radio systems with attackers," in *Proc. IEEE MILCOM,* 2017.

[15] X. Zhao, L. Li, S. Geng, H. Zhang, and Y. Ma, "A link-based variable probability learning approach for partially overlapping channels assignment on multi-radio multi-channel wireless mesh information-centric IoT networks," *IEEE Access*, vol. 7, pp. 45137–45145, 2019.

[16] L. Li, X. Zhao, S. Geng, and Y. Zhang, "An efficient partially overlapping channels assignment for smart grid IoT with differentiated QoS," *IEEE Access*, vol. 7, pp. 165207–165216, 2019.

[17] N. Abdeddaim, F. Theoleyre, F. Rousseau, and A. Duda, "Multi-channel cluster tree for 802.15.4 wireless sensor networks," in *Proc. IEEE PIMRC*, 2012.

[18] B. Kim and S. Kim, "An AHP-based interface and channel selection for multi-channel MAC protocol in IoT ecosystem," *Wireless Personal Commun.*, vol. 93, pp. 97–118, 2017.

[19] X. L. Huang, X. W. Tang, and F. Hu, "Dynamic spectrum access for multimedia transmission over multi-user, multi-channel cognitive radio networks," *IEEE Trans. Multimedia*, vol. 22, no. 1, pp. 201–214, 2020.

[20] X. L. Huang, Y. X. Li, Y. Gao, and X. W. Tang, "Q-learning-based spectrum access for multimedia transmission over cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 1, pp. 110–119, 2021.

[21] H. Salameh, "Resource management with probabilistic performance guarantees in opportunistic networks," *AEU - Int. J. Electronics Commun.*, vol. 67, no. 7, pp. 632–636, 2013.

[22] H. Salameh, "Probabilistic spectrum assignment for QoS-constrained cognitive radios with parallel transmission capability," in *Proc. IFIP Wireless Days,* 2013.

[23] H. A. Bany Salameh, S. Almajali, M. Ayyash, and H. Elgala, "Spectrum assignment in cognitive radio networks for Internet-of-things delay-sensitive applications under jamming attacks," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1904–1913, Jun. 2018.

[24] H. Bany Salameh, R. Tashtoush, H. Al-Obiedollah, A. Alajlouni, Y. Jararweh,"Power allocation technique with soft performance guarantees in hybrid OFDMA–NOMA cognitive radio systems: Modeling and simulation," *Simul. Model. Prac. Theory*, vol. 112, Nov. 2021.

[25] R. Halloush, H. B. Salameh, A. Musa, M. Halloush and M. A. Shunnar, "Highly reliable transmission and channel assignment for CR-IoT networks," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3945–3953, Mar. 2022.

[26] H. B. Salameh, M. Krunz, and D. Manzi, "Spectrum bonding and aggregation with guard-band awareness in cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 3, pp. 569–581, Mar. 2014.

[27] H. Bany Salameh, H. Kasasbeh, and B. Harb, "A batch-based MAC design with simultaneous assignment decisions for improved throughput in guard-band-constrained cognitive networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1143–1152, Mar. 2016.

[28] R. Pissard-Gibollet, E. Fleury, G. Harter, O. Fambon, and F. Saint-Marcel, "FIT IoT-LAB Tutorial: Hands-on practice with a very large scale testbed tool for the Internet of things," in *Proc. UbiMob,* 2014.

[29] M. H. Khadr, H. A. Bany Salameh, M. Ayyash, S. Almajali, and H. Elgala, "Securing IoT delay-sensitive communications with opportunistic parallel transmission capability,"in *Proc. IEEE GLOBECOM,* 2019.

[30] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer localization in multi-hop wireless network: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 765–799, 2017.

[31] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 2009.

[32] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. MobiHoc,* 2005.

[33] J. D. Poston and W. D. Horne, "Discontiguous OFDM considerations for dynamic spectrum access in idle TV channels," in *Proc. IEEE DySPAN,* 2005.

[34] Y. Wu, B. Wang, and K. J. R. Liu, "Optimal defense against jamming attacks in cognitive radio networks using the Markov decision process approach," in *Proc. IEEE GLOBECOM,* 2010.

[35] E. Bayraktaroglu, *et al.*, "On the performance of IEEE 802.11 under jamming," in *Proc. IEEE INFOCOM,* 2008.

[36] H. Bany Salameh, R. Qawasmeh and A. F. Al-Ajlouni, "Routing with intelligent spectrum assignment in full-duplex cognitive networks under varying channel conditions," *IEEE Commun. Letters*, vol. 24, no. 4, pp. 872–876, Apr. 2020.

[37] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A jammed-area mapping service for sensor networks," in *Proc. IEEE RTSS,* 2003.

[38] R. Muraleedharan and L. A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system," in *Proc. Wireless Sensing Processing*, 2006.

[39] S. K. Jain and K. Garg, "A hybrid model of defense techniques against base station jamming attack in wireless sensor networks," in *Proc. CICSYN,* 2009.

[40] A. Gluhak, *et al.*, "A survey on facilities for experimental Internet of things research," *IEEE Commun. Mag.*, vol. 49, pp. 58–67, Nov. 2011.

[41] J. Horneber and A. Hergenröder, "A Survey on testbeds and experimentation environments for wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1820–1838, 2014.

[42] M. Sharif and A. Sadeghi-Niaraki, "Ubiquitous sensor network simulation and emulation environments: a survey," *J. Netw. Comput. Appl.*, vol. 93, pp. 150–181, 2017.

[43] A-S. Tonneau, N. Mitton, and J. Vandaele, "How to choose an experimentation platform for wireless sensor networks? A survey on static and mobile wireless sensor network experimentation facilities," *Ad Hoc Netw.*, vol. 30, pp. 115–127, Jul. 2015.

[44] T. Watteyne, C. Adjih, and X. Vilajosana, "Lessons learned from large-scale dense IEEE 802.15.4 connectivity traces," in *Proc. IEEE CASE,* 2015.

[45] FIT IoT-LAB Lille site. Accessed: Apr. 5, 2022. [Online]. Available: https://www.iot-lab.info/docs/deployment/lille/

[46] E. Ahmed, A. Gani, S. Abolfazli, L. J. Yao, and S. U. Khan, "Channel assignment algorithms in cognitive radio networks: Taxonomy, open issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 795–823, 2016.
[47] W. Si, S. Selvakennedy, and A. Y. Zomaya, "An overview of channel assignment methods for multi-radio multi-channel wireless mesh networks," *J. Parallel Distrib. Comput.*, vol. 70, no. 5, pp. 505–524, 2010.
[48] AT86RF231 datasheet. Accessed: Apr. 25, 2022. [Online]. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/doc8111.pdf
[49] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. IEEE INFOCOM*, 2011.

Monette H. Khadr (M'17) received the MS.c degree and the BS.c degree in Electronics and communications engineering from the Arab Academy for Science, Technology, and Maritime Transport, Alexandria, Egypt in 2016 and 2007, respectively. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University at Albany SUNY, Albany, NY, USA, where she is a member of the Signals and Networks (SINE) Lab. Her research interests include machine learning based optimization of wireless systems, heterogeneous wireless networks, spectrum management and physical layer security.

Haythem Bany Salameh received the Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, Tucson, AZ, USA, in 2009. He is currently a Professor of Telecommunication Engineering with Al Ain University, Al Ain, UAE, and in leave from Yarmouk University, Irbid, Jordan. His research interests include wireless networking, with emphasis on dynamic spectrum access, cognitive radio networking, Internet-of-things, security, 5G networking, artificial intelligence, and distributed protocol design.

Moussa Ayyash (M'98–SM'12) received his B.S., M.S. and Ph.D. degrees in Electrical and Computer Engineering. He is currently a Professor at the Department of Computing, Information, and Mathematical Sciences and Technology, Chicago State University, Chicago. He is the Director of the Center of Information and Security Education and Research (CINSER). His current research interests span digital and data communication areas, wireless networking, visible light communications, network security, Internet of things, and interference mitigation. Dr. Ayyash is a member of the IEEE Computer and Communications Societies and a member of the Association for Computing Machinery. He is a recipient of the 2018 Best Survey Paper Award from IEEE Communications Society.

Hany Elgala (M'08) received the Ph.D. degree from Jacobs University, Germany, in 2010. He was a Research Professor with Boston University, USA. He is currently an Assistant Professor with the Electrical and Computer Engineering Department, University at Albany - State University of New York (SUNY), USA. He has authored or coauthored more than 100 journal and conference publications, several patents, and two book chapters. He has been active in optical wireless communications research for more than 15 years. His research interests include heterogeneous networks, machine learning for communications, and physical-layer security. He is currently an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS for Optical Wireless Systems and Networks.

Sufyan Almajali received the Ph.D. degree in Computer Science from the Illinois Institute of Technology, Chicago, IL, USA. He worked for several IT companies in USA, including the Director of Technology Solutions for Vertex, Chicago, the Chief Technology Officer with Secure Data Replicator, Chicago, where he supervised the development of an online real-time data replication system. He has 21 years of academic and industrial experience. He is currently an Associate Professor of Computer Science with Princess Sumaya University for Technology, Amman, Jordan. In addition to Princess Sumaya University, he taught at several universities in the states, including Chicago State University, Robert Morris University, DeVry University, and Benedictine University. His current research interests include the Internet of things security, mobile edge computing, and network security.