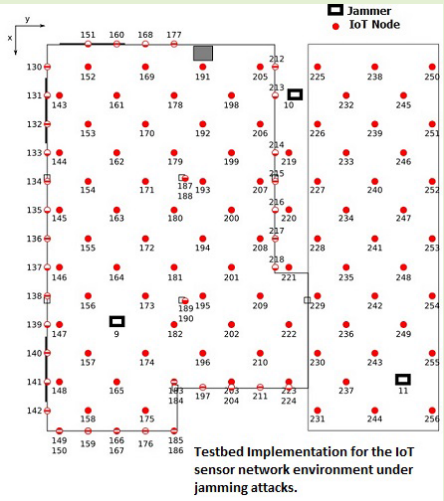
# Jamming-Aware Simultaneous Multi-Channel Decisions for Opportunistic Access in Delay-Critical IoT-Based Sensor Networks

Haythem A. Bany Salameh, *Senior Member, IEEE*,
Monette H. Khadr, *Graduate Student Member, IEEE*,
Mohammad Al-Quraan, *Student Member, IEEE*, Moussa Ayyash, *Senior Member, IEEE*,
Hany Elgala, *Member, IEEE*, and Sufyan Almajali, *Member, IEEE*

***Abstract*—Cognitive radio (CR) technology is proposed to provide huge spectrum opportunities to enable a large-scale deployment of Internet-of-Things (IoT) sensing-based applications. An important challenge in this domain is how to design efficient channel assignment algorithms for delay-sensitive CRIoT-based sensor networks while being resilient to jamming attacks (the most common threat to IoT network reliability). Such channel assignment algorithms must enable parallel multi-channel transmissions in order to satisfy the imposed quality-of-service and delay requirements of the CRIoT devices while being spectrum efficient. This article introduces a multi-channel batch-based security-aware medium access control (MAC) design proposed for time-critical CRIoT deployments, referred to as BMRJA-MAC. The proposed design aims at improving the overall network performance by serving the largest possible number of CRIoT nodes by utilizing their multi-channel transmission capabilities while being reactive jamming-aware. The performance of the proposed MAC design is validated via simulations and experimentally using the Future Internet-of-Things (FIT) IoT-LAB testbed. Compared with reference protocols, the results show that BMRJA-MAC significantly improves network performance and spectrum efficiency.**




***Index Terms*—Cognitive radio (CR), Internet-of-Things (IoT), reactive jamming, spectrum assignment, testbed, CRIoT.**

## I. Introduction

INTERNET-OF-THINGS (IoT) has become the keyword to describe the connectivity of numerous devices such as sensing devices to the Internet. In addition to connectivity, IoT presents its challenges when it comes to connectivity, security and data storage needs [1]. Many IoT sensor networks consist of a large number of mobile nodes that rely on diverse enabling wireless technologies for connectivity needs [2]–[5]. Serving a massive number of deployed IoT devices will magnify the frequency spectrum crunch [6]–[8]. Cognitive radio (CR) technology provides a solution for IoT networks to improve spectrum usage through dynamic spectrum access [9]. IoT-based sensor networks with CR-capability are referred to as (CRIoT). In CRIoT, unlicensed secondary users (SUs) share the channels with nodes that act as licensed primary users (PUs). SUs are given access to the unused channels given that they do not interfere with PU transmissions.

Due to the complexity of IoT networks, security issues can lead to dramatic impacts on private and public networks. One local vulnerability can lead to major cyber attacks on the Internet as a whole [10]. An important security concern in IoT networks is related to jamming attacks. Jamming attacks can limit users from accessing shared wireless channels or damage packets in transmission. In wireless communications, jamming attacks are the common threat to the reliability of

Manuscript received October 14, 2021; revised November 17, 2021; accepted December 15, 2021. Date of publication December 20, 2021; date of current version January 31, 2022. The associate editor coordinating the review of this article and approving it for publication was Prof. Houbing Song. *(Corresponding author: Haythem A. Bany Salameh.)*

Haythem A. Bany Salameh is with the College of Engineering, Al Ain University, Al Ain, United Arab Emirates, and also with the Department of Telecommunications Engineering, Yarmouk University, Irbid 21163, Jordan (e-mail: haythem.banysalameh@aau.ac.ae).

Monette H. Khadr and Hany Elgala are with the Electrical and Computer Engineering Department, University at Albany, Albany, NY 12222 USA (e-mail: mkhadr@albany.edu; helgala@albany.edu).

Mohammad Al-Quraan is with the Department of Telecommunications Engineering, Yarmouk University, Irbid 21163, Jordan, and also with the School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K.

Moussa Ayyash is with the Department of Computing, Information, and Mathematical Sciences & Technology, Chicago State University, Chicago, IL 60628 USA (e-mail: msma@ieee.org).

Sufyan Almajali is with the Computer Science Department, Princess Sumaya University for Technology, Amman 11941, Jordan (e-mail: s.almajali@psut.edu.jo).

Digital Object Identifier 10.1109/JSEN.2021.3136640

the wireless network [11]. Therefore, developing jamming resilient algorithms is crucial in wireless IoT networks. Jamming attacks are generally caused by proactive jammers or reactive jammers. A proactive jammer follows a predefined strategy to disrupt ongoing transmissions. On the other hand, a reactive jammer can intelligently predict CR users' transmission and it then sends the jamming traffic accordingly. In the case of time-critical applications in CRIoTs, such as telesurgery, packet transmission delay and throughput are crucial performance metrics and must be taken into consideration. Whenever a packet suffers a transmission delay of more than a predefined threshold value, it is considered obsolete. In this paper, a jamming-aware simultaneous multi-channel assignment solution for delay-critical IoT applications is developed. The proposed solution allows the CRIoT devices to utilize the idle PU channels while being aware of the prevailing jamming attacks and PU activities such that a set of quality of service (QoS) requirements are satisfied. This work introduces a batch-based multi-channel reactive jamming-aware MAC (BMRJA-MAC) protocol. BMRJA-MAC considers the unique characteristics of CRIoT networks in terms of PU activity, channel conditions, jamming attack levels, and QoS requirements for delay-critical IoT applications. The proposed protocol enhances network performance by simultaneously allocating multiple channels for multiple CRIoT communicating pairs while being aware of the reactive jamming attacks over the different PU channels. The key contributions are:

- Mathematical modeling of the batch-based multi-channel assignment problem that considers channel conditions, PUs activity, delay, and QoS requirements while resisting reactive jamming attacks. The derived solution turned out to be a non-linear binary problem (NLBP).
- Mathematical manipulations to linearize the NLBP problem. Also, the sequential-fixing linear-programming (SFLP) method [12] is used as a tool to obtain polynomial-time sub-optimal solutions.
- The proposed algorithm is extensively investigated via simulations to study its performance under various conditions including jamming severity, number of users, rate demands, PU activity, and number of transceivers.
- The simulation results are experimentally validated using real-life experiments which are orchestrated to mimic practical deployment settings on a large-scale testbed, the Future Internet-of-Things (FIT) IoT-LAB [13].

Note that our proposed protocol has several applications in medical networks. This includes applications that require patients' mobility with a minimum delay of data delivery (i.e., IoT-based remote patient monitoring systems). Several real-time health readings (e.g., blood pressure, heart rate) can be read via wearable IoT devices and reported back to physicians/hospitals. The sensitivity of the delay is very high in such applications as immediate actions should be taken in emergency cases.

The rest of the paper is structured as follows. Section II summarises the related work. Section III presents preliminaries, Section IV elaborates in detail the channel assignment problem, Section V covers the channel access and Section VI discusses the simulation/test-bed results. Section VII concludes the paper.

## II. Related Work

There is a number of protocols and mechanisms that have been proposed for maximizing spectrum utilization in CR-based networks (e.g., [9], [14]). In [9], a multi-channel assignment scheme for ad hoc CR networks (CRNs) was presented as a channel selection algorithm with spectrum aggregation to improve network throughput while maintaining fairness. A capacity-aware spectrum allocation model for CRNs that simultaneously serves multiple CR devices with the objective of maximizing network capacity while considering QoS parameters was proposed in [14]. Only a few efforts in the literature consider jamming attacks while aiming at maximizing spectrum efficiency. Efforts include a channel-hopping based approach in [15], a game-theory approach in [16], a deep reinforcement machine learning method in [17], and a Particle Bee convolution neural-network cross-layer design in [18]. Neither of these algorithms was designed for delay-critical applications, nor they serve multiple CRIoT devices or allow for multiple-channel transmissions. A near-optimal energy-efficient jamming-aware learning algorithm was proposed for CRNs that allows each SU to execute sensing, joint data aggregation, channel probing, and spectrum access [19]. The algorithm selects the least jammed, or ideally un-jammed, channels to access without knowing the jamming behaviour, type of PUs and channel accessibility conditions. Yet, it is not investigated for delay-critical applications nor serve multiple CR nodes concurrently. For time-critical single-channel CRIoT transmissions, a multi-channel jamming-aware channel assignment protocol, referred to as security-aware multi-channel MAC (SAMC-MAC) protocol was proposed in [20]. The algorithm allows parallel transmission of CRIoT devices for delay-sensitive applications. It is a batch-based approach that chooses the best channel/channels (based on the invalidity ratio metric) for a group of CRIoT communicating pairs while considering delay requirements, link quality, PU activity and jamming attack severity. However, it is limited to proactive jamming mitigation. SAMC-MAC was compared with reference jamming-aware channel assignment variants including parallel-channel security-aware MAC (PCS-MAC) protocol with no simultaneously decisions, batching-based single-channel security-aware MAC protocol with no parallel transmission capabilities [20], and single-channel security-aware MAC protocol. SAMC-MAC improved the performance over the other protocols.

In summary, most of the existing parallel-channel CR assignment techniques make their decisions without considering other CR users. They solely decide based on a per-link sequential greedy approach without considering the impact of jamming attacks. On the other hand, most existing jamming-aware spectrum assignment approaches were designed based on either sacrificing network resources (e.g., power, complexity, and spectrum) or requiring dedicated hardware to detect and mitigate jamming attacks. These approaches were not designed for delay-critical applications. A few jamming-aware channel assignment protocols were designed for delay-critical IoT networks without the need for extra resources. However, these protocols cannot simultaneously serve multiple CRIoT pairs and/or are limited to proactive jamming mitigation. In addition, most of these efforts were verified

using simulations with no real-life testbed validation. Unlike most previous works, we focus on designing a service-oriented multi-channel assignment to satisfy the QoS requirements of IoT applications. To the best of our knowledge, it is the first work to use a hardware-based testbed to implement and verify the performance of a reactive jamming-aware protocol with parallel transmission capability in CRIoT networks.

## III. Preliminaries

### A. Network Model

We assume that we have a single-hop network of CRIoT devices that coexists geographically with different licensed PUs. The CRIoT devices are within the transmission range of each other and communicate based on multi-channel carrier-sense medium-access with collision-avoidance (CSMA/CA)-based access mechanism. The licensed spectrum of the PU networks consists of $M = |\mathcal{M}|$ adjacent orthogonal channels, where $\mathcal{M}$ is the set of all PU channels. A 2-state IDLE/BUSY Markov renewal process models the status of each PU channel $i \in \mathcal{M}$. The busy- and idle-periods of each channel $i$ are respectively given by the random processes $T_B^{(i)}$ and $T_I^{(i)}$. The arrival rate of PU users over each channel $i$ is a Poisson process, in which the idle- and busy-period rates are $1/\overline{T}_I^{(i)}$ and $1/\overline{T}_B^{(i)}$, respectively. Note that the idle PU channels are allowed to be opportunistically utilized by the CRIoT devices. A CRIoT transmitter transmits over a selected idle channel $i$ using the maximum permissible power mask $P_{\max}^{(i)}$ enforced by the federal communication commission. An idle channel can be utilized as long as the received signal-to-noise-ratio over that channel exceeds a pre-specified threshold. Each CRIoT device $j$ has $L_{x_j}$ transceivers and requires a rate demand of $R_{D_j}$ Mbps with data packet size of $L_j$ bits. We assume that there is a common control channel that can be used by the CRIoT users to share their transmission information and to coordinate their transmissions. An exclusive channel occupancy is adopted by the CRIoT devices, in which only one transmission can utilize an idle channel at a given time.

### B. Reactive Jamming and Packet-Invalidity Ratio Analysis

The main categories of jammers include constant, deceptive, proactive/random, and reactive [21]. 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 [22]. 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 above two attacks require a significant amount of power. Proactive jammers alternate between sleeping and jamming phases irrespective of CRIoT activities [23]. Reactive jammers, on the other hand, are the most energy-efficient types of attacks, as they transmit only when a CRIoT signal is detected. This work focuses on reactive jamming attacks.

For reactive jamming, the condition for successful packet delivery occurs when the total required transmission period of the CRIoT packet is less than the idle period of the selected channel and no jamming to impact the packet occurs during that time. To ensure that the packet was not damaged by the jammer, for a given assignment $\Omega = \{m_1, m_2, \ldots, m_M\}$, the failure probability for CRIoT user $j$ can be given as [23]:

$$p_{f_j} = \left(1 - \prod_{i \in \Omega} e^{-\frac{t_{x_j}}{\overline{T}_I^{(i)}}} (1 - P_J^{(i)})\right)^{N_x} \tag{1}$$

where $P_J^{(i)}$ is the jamming probability over channel $i$, $t_{x_j} = \frac{L_j}{\sum_{i \in \Omega} R_j^{(i)}}$, $R_j^{(i)}$ denotes the achieved transmission rate of CRIoT transmission $j$ over the $i$th channel and $N_x$ represents number of packet retransmission. For reactive jamming, the packet-invalidity ratio (PIR), $r_j$, is derived in [23] as follows:

$$r_j \leq \frac{p_{f_j} \overline{d_k}}{(1 - p_{f_j})(D_{th} - \overline{d_k}) + p_{f_j} \overline{d_k}} \tag{2}$$

where $D_{th}$ is the maximum allowed delay; if the transmission delay exceeds $D_{th}$, this packet transmission is considered as invalid. $d_k$ denotes the delay due to the $k^{\text{th}}$ re-transmission attempt and $\overline{d_k}$ represents the average MAC layer delay. For a PIR requirement $\gamma$, *i.e.,* $(r_j \leq \gamma)$, Eq. (2) can be written as:

$$p_{f_j} \leq \frac{\gamma\,(D_{th} - \overline{d_k})}{(\,\overline{d_k}(1 - 2\gamma) + \gamma\, D_{th}\,)} = B_{th}^{(D_{th}, \gamma, \overline{d_k})} \tag{3}$$

where $B_{th}$ is a threshold-dependent delay constant. Substituting (1) in (3) and after some mathematical manipulations, we get:

$$\ln(1 - \sqrt[N_x]{B_{th}}) \leq \sum_{i \in \Omega} \left(\ln(1 - P_J^{(i)}) - \frac{t_x}{\overline{T}_I^{(i)}}\right) \tag{4}$$

## IV. Optimal Channel Assignment Problem

### A. Problem Statement and Constraints

For a set of competing CRIoT devices $\mathcal{N}$, per-user rate-demand, available channel list, perceivable data rate over each idle channel, the PU activities, the delay requirement and the reactive jamming severity parameters over the various idle channels, we aim at finding a suitable channel assignment aiming to simultaneously serve the largest possible number of CRIoT transmissions subject to:

*C1. The QoS Constraints:* The required CRIoT rate demand $R_{D_j}$ is achieved with a packet invalidity ratio that is less than $\gamma$ ($\gamma$ is computed such that a delay requirement $D_{th}$ is achieved).

*C2. Exclusive-Channel Occupancy and Number of Transceivers Constraints:* A channel is not to be assigned to more than one CRIoT device at the same time and the total assigned channels for each CRIoT transmission is at most $L_x$ ($\leq$ the number of available transceivers).

### B. Problem Formulation

Recall that we seek finding the channel assignment that achieves the design objective of maximizing the number of simultaneously admitted CRIoT devices with achieved design constraints. To this end, we define a decision 0/1-variable $\alpha_j^{(i)}$ for each CRIoT transmission $j \in \mathcal{N}$ over every channel $i$ as:

$$\alpha^{(i)} = \begin{cases} 1, & \text{if channel } i \text{ is allocated to CRIoT } j \\ 0, & \text{otherwise.} \end{cases}$$

Using the defined decision variables $\alpha$'s, our objective function $O(\alpha_j^{(i)})$ can be written as:

$$O(\alpha_j^{(i)}) = \sum_{j\in\mathcal{N}} 1[\sum_{i\in\mathcal{M}} \alpha_j^{(i)}] + \frac{\sum_{j\in\mathcal{N}}\sum_{i\in\mathcal{M}} \alpha_j^{(i)} R_j^{(i)}}{\sum_{i\in\mathcal{M}} R_j^{(i)}} \quad (5)$$

where 1[.] is the indicator function. Note that the first term of $O(\alpha_j^{(i)})$ represents the number of admitted CRIoT transmissions while the second term, which is always $< 1$, is used to break the tie between any two assignments with the same number of served CRIoT devices by selecting the assignment that provides higher total sum-rate. Following the same methodology used in [20], the non-linear term (i.e., the indicator function) in the objective can be linearized by defining the variable $U_j = 1[\sum_{i\in\mathcal{M}} \alpha_j^{(i)}]$, $\forall j \in \mathcal{N}$ and adding two constraints as:

$$\frac{1}{M}\sum_{i\in\mathcal{M}} \alpha_j^{(i)} - U_j \le 0, \quad \forall j \in \mathcal{N}$$
$$U_j - \sum_{i\in\mathcal{M}} \alpha_j^{(i)} \le 0, \ \forall j \in \mathcal{N}. \quad (6)$$

Therefore, $O(\alpha_j^{(i)})$ becomes:

$$\max \sum_{j\in\mathcal{N}} U_j + \frac{\sum_{j\in\mathcal{N}}\sum_{i\in\mathcal{M}} \alpha_j^{(i)} R_j^{(i)}}{\sum_{i\in\mathcal{M}} R_j^{(i)}}. \quad (7)$$

Using the introduced binary variables, the rate demand constraints can be written as:

$$\sum_{i\in\mathcal{M}} R_j^{(i)}\alpha_j^{(i)} \ge R_{D_j} \text{ or } \sum_{i\in\mathcal{M}} R_j^{(i)}\alpha_j^{(i)} = 0, \quad \forall j \in \mathcal{N}.$$

This constraint can be written in a linear form as:

$$\sum_{i\in\mathcal{M}} -R_j^{(i)}\alpha_j^{(i)} - \Psi y_1^{(j)} \le -R_{D_j}, \quad \forall j \in \mathcal{N}$$
$$\sum_{i\in\mathcal{M}} R_j^{(i)}\alpha_j^{(i)} - \Psi y_2^{(j)} \le 0, \quad \forall j \in \mathcal{N}$$
$$y_1^{(j)} + y_2^{(j)} = 1, \quad \forall j \in \mathcal{N}. \quad (8)$$

Writing the invalidity-ratio in (4) in terms of $\alpha_j^{(i)}$ variables, the invalidity-ratio constraint can be expressed as:

$$\sum_{i=1}^{M} \Big(\ln(1 - \sqrt[N_x]{B_{th}})\overline{T}_I^{(i)} R_j^{(i)} + L_j\Big)\alpha_j^{(i)} \le \sum_{i=1}^{M}\sum_{k=1}^{M} \ln(1 - P_J^{(i)})\overline{T}_I^{(i)} R_j^{(k)} \alpha_j^{(i)}\alpha_j^{(k)} \quad (9)$$

After some mathematical steps, (9) can be rewritten as:

$$\sum_{i=1}^{M} b_j^{(i)}\alpha_j^{(i)} \le \sum_{j=1}^{M}\sum_{k=1}^{M} c_j^{(ik)}\alpha_j^{(i)}\alpha_j^{(k)} \quad (10)$$

where $b_j^{(i)} = \ln(1 - \sqrt[N_x]{B_{th}})R_j^{(i)} + L_j$, $c_j^{(ik)} = \ln(1 - P_J^{(i)})$ $R_j^{(k)}$, $\forall j \in \mathcal{N}, i, k \in \mathcal{M}$. The invalidity-ratio constraint in (10) seems to be non-linear that is hard to optimize. To linearize (10), we introduce a new binary parameter $w_j^{(ik)} = \alpha_j^{(i)}\alpha_j^{(k)}$ and add the following three constraints:

$$w_j^{(ik)} \le \alpha_j^{(i)}, \quad \forall j \in \mathcal{N}, \ i, k \in \mathcal{M}$$
$$w_j^{(ik)} \le \alpha_j^{(k)}, \quad \forall j \in \mathcal{N}, \ i, k \in \mathcal{M}$$
$$w_j^{(ik)} \ge \alpha_j^{(i)} + \alpha_j^{(k)} - 1 \quad \forall j \in \mathcal{N}, \ i, k \in \mathcal{M} \quad (11)$$

The exclusive-channel occupancy and number of utilized channels constraints can be respectively written in terms of $\alpha_j^{(i)}$ as:

$$\sum_{j\in\mathcal{N}} \alpha_j^{(i)} \le 1, \quad \forall i \in \mathcal{M} \text{ and } \sum_{i\in\mathcal{M}} \alpha_j^{(i)} \le L_{x_j}, \ \forall j \in \mathcal{N} \quad (12)$$

Given the objective function in (7) and the design constraints in (6), (8), (11) and (12), our optimization can be expressed as:

$$\max \sum_{j\in\mathcal{N}} O(\alpha_j^{(i)}) = U_j + \frac{\sum_{j\in\mathcal{N}}\sum_{i\in\mathcal{M}} \alpha_j^{(i)} R_j^{(i)}}{\sum_{i\in\mathcal{M}} R_j^{(i)}}$$
$$\text{s.t. } U_j - \sum_{i\in\mathcal{M}} \alpha_j^{(i)} \le 0, \quad \forall j \in \mathcal{N}$$
$$\frac{1}{M}\sum_{i\in\mathcal{M}} \alpha_j^{(i)} - U_j \le 0, \quad \forall j \in \mathcal{N}$$
$$\sum_{i\in\mathcal{M}} b_j^{(i)}\alpha_j^{(i)} - \sum_{i\in\mathcal{M}}\sum_{k\in\mathcal{M}} c_j^{(ik)} w_j^{(ik)} \le 0, \quad \forall j \in \mathcal{N}$$
$$\sum_{i\in\mathcal{M}} -R_j^{(i)}\alpha_j^{(i)} - \Psi y_1^{(j)} \le -R_{D_j}, \quad \forall j \in \mathcal{N}$$
$$\sum_{i\in\mathcal{M}} R_j^{(i)}\alpha_j^{(i)} - \Psi y_2^{(j)} \le 0, \quad \forall j \in \mathcal{N}$$
$$y_1^{(j)} + y_2^{(j)} = 1, \quad \forall j \in \mathcal{N}$$
$$w_j^{(ik)} \le \alpha_j^{(i)}, \quad \forall j \in \mathcal{N}, i, k \in \mathcal{M}$$
$$w_j^{(ik)} \le \alpha_j^{(k)}, \quad \forall j \in \mathcal{N}, \ i, k \in \mathcal{M}$$
$$w_j^{(ik)} \ge \alpha_j^{(i)} + \alpha_j^{(k)} - 1, \quad \forall j \in \mathcal{N}, i, k \in \mathcal{M}$$
$$\sum_{j\in\mathcal{N}} \alpha_j^{(i)} \le 1, \quad \forall i \in \mathcal{M}$$
$$\sum_{i\in\mathcal{M}} \alpha_j^{(i)} \le L_{x_j} \quad \forall j \in \mathcal{N}.$$

The formulated optimization problem is a binary linear problem (BLP), which is a *combinatorial* multi-channel multi-user matching problem. The optimal solution of such a combinatorial optimization can be obtained through an exhaustive search of all possible combinations of channel-user assignments, which exponentially grows with the number of contending CRIoT devices $N = |\mathcal{N}|$ and PU channels $M$. Thus, our formulated channel assignment matching problem is NP-hard (i.e., matching problems have been previously proven to be NP-hard [24]). There are a number of approximate algorithms for solving such problems including: cutting-plane, branch-and-bound and decomposition methods [25]. However, their worst-case time complexity is still exponential as $N$ and $M$ increase [26]. To obtain sub-optimal solutions for our problem in polynomial-time, the SFLP procedure is adopted. This procedure has been adopted by several existing research efforts

to solve similar BLP problems, by which suboptimal solutions with polynomial-time complexity were demonstrated [12]. The adopted SFLP methodology is executed as follows:

*Step 1:* All unfixed variables are relaxed to real numbers in [0, 1] range, resulting in a relaxed linear programming (LP).

*Step 2:* The relaxed LP problem is solved using the polynomial-time standard LP methods. If the LP is infeasible, then no feasible solution can be found for the original BLP. Otherwise, the CRIoT communicating pair with the highest summation of $\alpha$'s among the $N$ CRIoT pairs is identified.

*Step 3:* The decision variable with the highest value among all unfixed $\alpha$'s of the identified CRIoT pair is set to 1. The LP is then updated and resolved with the fixed $\alpha$'s. If infeasible, the fixed $\alpha$ is not correct and should be 0.

*Step 4:* The process in Step 3 is repeated until the QoS requirements for the identified CRIoT pair is either met or all $\alpha$'s of that pair are fixed without meeting its requirements. In the latter case, this pair is blocked and all of its $\alpha$'s are fixed to 0. Otherwise, only the unfixed $\alpha$'s of that pair are set to 0.

*Step 5:* Find the next not yet served CRIoT pair with the highest summation of unfixed $\alpha$'s. The optimization Steps 3-5 are then repeated for the newly identified pair while accounting for already fixed decision variables.

*Step 6:* The process in Step 5 is repeated until each of the $N$ CRIoT pairs is either assigned a set of channels to serve its QoS demands or no feasible assignment can be found.

## V. Admission Control and Spectrum Access Protocol

To realize our channel assignment algorithm in a distributed way, the multi-channel IEEE 802.11-based distributed CRN MAC protocol in [27] is adopted, which implements a common control channel (CCC) approach. This MAC protocol allows multiple CRIoT devices to exchange their control information and perform simultaneous channel assignment decisions. This is realized based on introducing an Access Window (AW) admission control procedure, during which all CRIoT communicating pairs exchange their request-to-send (RTS) and clear-to-send (CTS) control packets. The sequence of exchanged control packets disseminates all the required information to perform our channel assignment algorithm. Specifically, the exchanged control information are available to all contending CRIoT devices as they belong to a single-hop network (i.e., the devices are within the range of each other). Given the exchanged control information, the device-channel assignment decisions are simultaneously conducted by the contending CRIoT devices according to our proposed channel assignment algorithm in Section IV.B. We note that the channel assignment decisions are cooperatively made by the contending CRIoT communicating pairs, and hence the overall achieved network throughput is enhances.

## VI. Performance Evaluation

A CRIoT network that coexists with different PU networks in the same geographical area is considered. It is assumed that there is no online interaction between the different networks. The CRIoT network consists of $N$ communicating pairs that opportunistically utilize 10 PU channels. The CRIoT traffic is characterized as delay-sensitive, in which a data packet of length $L = 2$ kB is obsolete if it is not received within the delay threshold requirement ($D_{th} =$ 20ms) [20]. We set the MAC layer delay to $\overline{d_k} = 1$ ms, the number of permitted re-transmissions to $N_x = 4$, and the threshold $\gamma$ to 0.1. The idle durations ($\overline{I_I}^{(i)}$) over the 10 PU channels are {5, 100, 30, 5, 45, 50, 100, 5, 45, 30} ms. Achievable channel rates by the CRIoT users $R_j^{(i)}$ are randomly determined to be between 2 and 16 Mbps. We set the probability of jamming for the various PU channels to $\{0.06, 0.75, 0.03, 0.15, 0.015, 0.06, 1, 0.105, 0.015, 0.75\} \times X$, where $0 \leq X \leq 1$ is the jamming severity factor. Network throughput is our key performance metric, which is investigated under different jamming severity levels, PU activity levels, rate demand requirements $R_D$ and number of transceivers $L_x$. We conduct our simulations using MATLAB R2019 programs.

### A. Simulation Results

We investigate the performance of our proposed BMRJA-MAC for delay-critical CRIoT applications under reactive jamming attacks under different PU activity and jamming severity levels. Specifically, the performance of BMRJA-MAC is compared to that of two other MAC protocols: batch-based multi-channel reactive jamming-unaware MAC (BMRJU-MAC) and batch-based single-channel reactive jamming-aware MAC (BSRJA-MAC) [20]. The BSRJA-MAC protocol uses only one transceiver ($L_x = 1$), so each CRIoT can be allocated only a single channel. For the other two protocols, we set $L_x = 2$.

Figure 1 shows network throughput under low, moderate and high idle probability for different $R_D$. This figure indicates that network throughput decreases as $R_D$ increases as the chances of finding channels with higher rates decreases when increasing $R_D$. Under moderate-to-light jamming, our protocol outperforms BSRJA-MAC. This is expected because of the parallel transmission capability of our proposed protocol that allows the CRIoT devices to simultaneously utilize multiple channels. Under severe-to-moderate jamming attacks, our protocol shows better performance over BMRJU-MAC due to its inherent jamming awareness. While at light jamming attacks, the two protocols provide comparable performance as the jamming impacts becomes less dominant.

Network throughput for different $P_I$ and $R_D$ is depicted in Fig. 2. This figure exhibits that BMRJA-MAC provides an improved performance over BMRJU-MAC under severe-to-moderate jamming. However, under light jamming, the two protocols give the same performance because the impacts of jamming become less dominant. Also, Fig. 2 shows that the performance of BMRJA-MAC outperform that of the BSRJA-MAC under moderate-to-light jamming because of its parallel transmission capability. Note that under severe jamming attacks, the two protocols depict comparable performance under high PU activities. In general, as $P_I$ increases the achieved throughput increases because of the more availability of idle PU channels. Under severe jamming, throughput performance degrades for all protocols under low values of $P_I$. At severe-to-moderate jamming, the achieved throughput when $R_D = 8$ Mbps is higher than that when $R_D = 16$ Mbps. This is because the chances of finding channels that satisfy

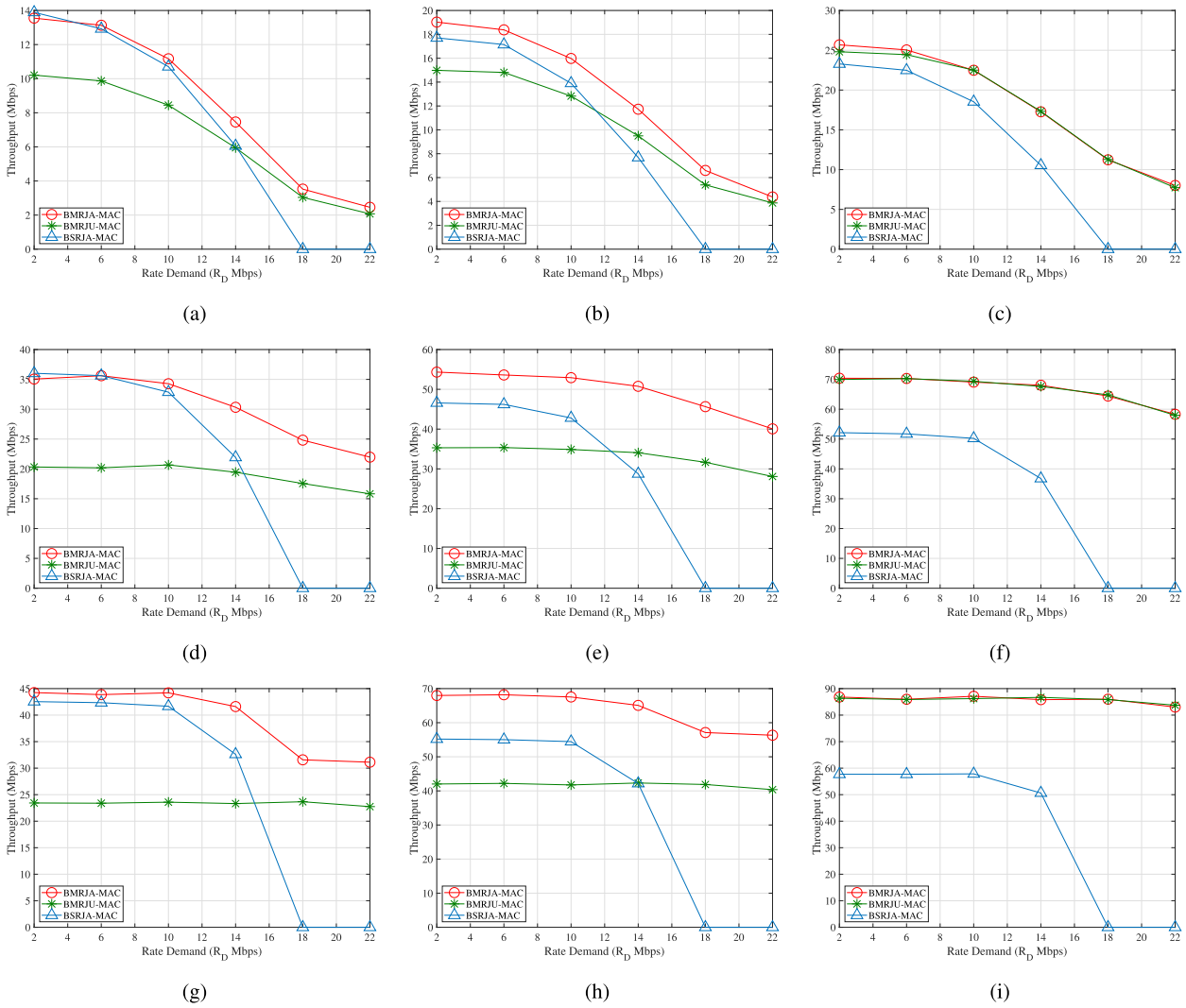



Fig. 1. Throughput performance *vs.* $R_D$ for $N = 5$ and $M = 10$ under (a) Severe attacks with $P_I = 0.1$, (b) Moderate attacks with $P_I = 0.1$, (c) Low-severity attacks with $P_I = 0.1$, (d) Severe attacks with $P_I = 0.1$, (e) Moderate attacks with $P_I = 0.5$, (f) Low-severity attacks with $P_I = 0.5$, (g) Severe attacks with $P_I = 0.9$, (h) Moderate attacks with $P_I = 0.9$, and (i) Low-severity attacks with $P_I = 0.9$.

the CRIoT QoS demand when $R_D = 8$ Mbps are higher than that when $R_D = 16$ Mbps.

Fig. 3 plots network throughput versus the number of CRIoT devices ($N$). This figure shows that our proposed protocol outperforms both BSRJA-MAC and BMRJU-MAC protocols. In general, as $N$ increases, network throughput improves. Fig. 3 also shows that as $P_I$ increases, network throughput increases. This is because the number of available idle channels increases. Also, if the jamming severity decreases the number of idle channels increases, which enhances throughput performance. We observe that the performance for $R_D = 8$ Mbps is better than that for $R_D = 16$ Mbps at $P_I = 0.1$. This is because of the limited number of idle channels. Fig. 3 also shows that for $P_I = 0.5$ and 0.9 under moderate-to-light attacks, the network throughput of our protocol and BMRJU-MAC is approximately the same for the two rate demands. For $R_D = 8$ Mbps, the two protocols serve more CRIoT devices with less per-user rate, while for $R_D = 16$ Mbps, fewer CRIoT devices are served with higher per-user rate, thus the achieved throughput is approximately the same. In BSRJA-MAC, the performance of $R_D = 8$ Mbps case outperforms that of the $R_D = 16$ Mbps case. This is because BSRJA-MAC can only use one channel, and hence the chances of finding a channel with rate of 16 Mbps is very low. When there are few number of idle channels, our protocol and BSRJA-MAC protocol achieve comparable performance. This is because of the low availability of idle channels, and hence the two protocols tend to utilize only one channel per CRIoT device.

Figure 4 illustrates network throughput versus jamming severity factor $X$ for $R_D = 8$ and 16 Mbps. This figure shows that BMRJA-MAC outperforms the other two protocols. This is because of its inherent jamming awareness and parallel transmission capability. It is clear that as the jamming severity increases, network throughput degrades for all protocols. Figure 4 also shows that network throughput for $R_D = 8$ Mbps is higher than that for $R_D = 16$ Mbps. This is because the probability of finding channels with transmission rate of 8 Mbps is higher than that of finding channels with a transmission rate of 16 Mbps, which results in serving more CRIoT devices with higher overall network throughput. Fig. 5 plots network throughput versus the number of per-device transceivers for $P_I = 0.1, 0.5$, and 0.9. It is obvious that

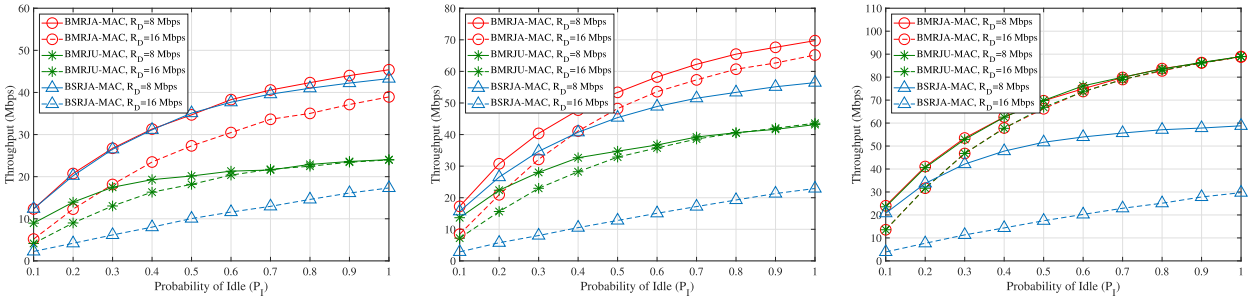



Fig. 2. Throughput performance *vs.* $P_I$ at $N = 5$ under (a) Severe attacks, (b) Moderate attacks, and (c) Light attacks.

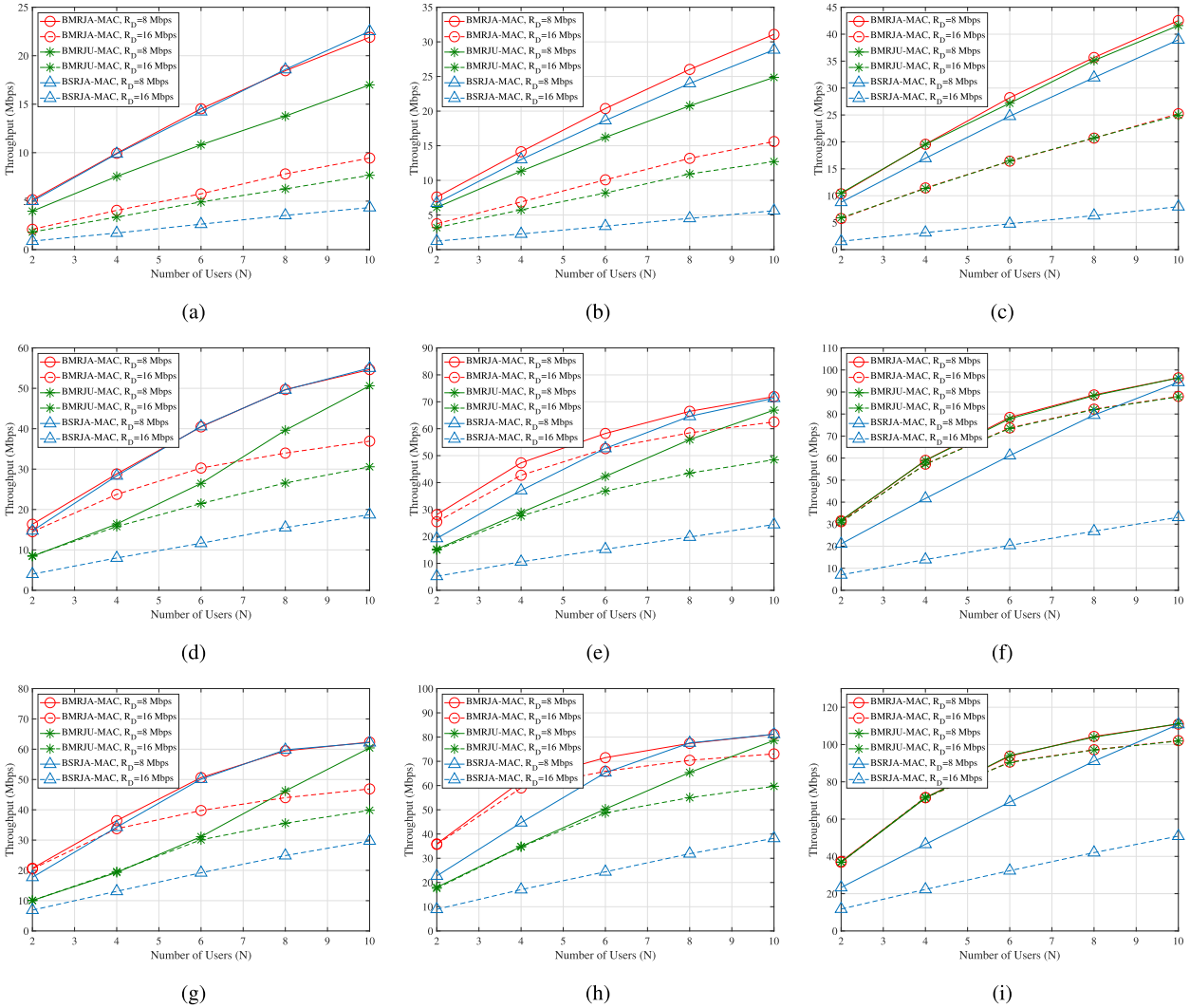



Fig. 3. Throughput performance *vs.* $N$ for different $R_D$ under (a) Severe attacks with $P_I = 0.1$, (b) Moderate attacks with $P_I = 0.1$, (c) Light attacks with $P_I = 0.1$, (d) Severe attacks with $P_I = 0.1$, (e) Moderate attacks with $P_I = 0.5$, (f) Light attacks with $P_I = 0.5$, (g) Severe attacks with $P_I = 0.9$, (h) Moderate attacks with $P_I = 0.9$, and (i) Light attacks with $P_I = 0.9$.

the throughput performance of BMRJA-MAC outperforms that of BMRJU-MAC. This figure reveals that throughput performance is approximately the same when $L_x \geq 2$, irrespective of $P_I$. This is because our main objective is to serve the largest possible number of CRIoT transmissions, and hence our protocol attempts to serve each transmission with the least number of channels (the chances of utilizing more than 2 channels is very small). Fig. 5 also indicates that under moderate-to-low jamming, using $L_x \geq 2$ achieves higher throughput compared to the case of $L_x = 1$. This is because of the higher availability of idle channels, in which each CRIoT device can utilize multiple channels to enhance network throughput. Under severe-to-moderate jamming, network throughput for $R_D = 8$ Mbps is better than that for $R_D = 16$ Mbps.

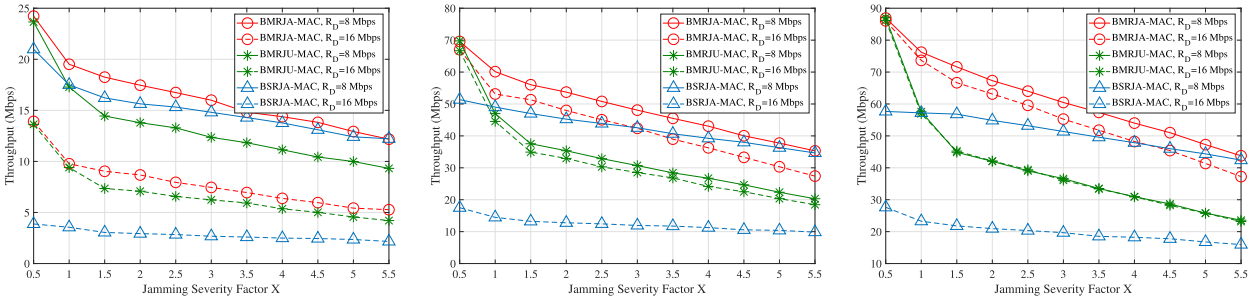



Fig. 4. Throughput performance *vs.* the jamming severity factor for various $R_D$ and $N = 5$ given (a) Low $P_I$ (High PU levels), (b) Moderate $P_I$ (Moderate PU levels), and (c) High $P_I$ (Low PU levels).

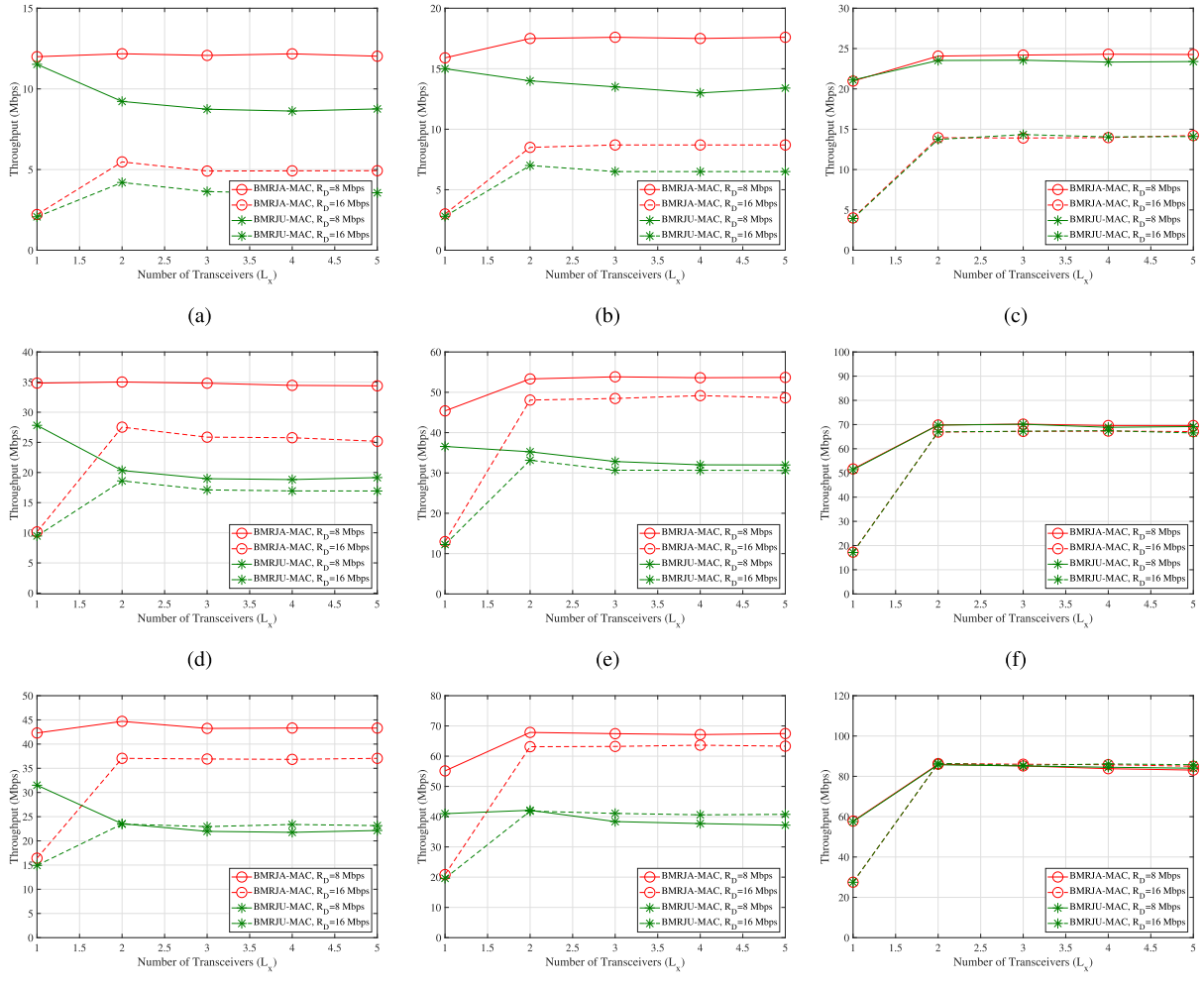



Fig. 5. Throughput performance *vs.* $L_x$ for various $R_D$, $N = 5$ and $M = 10$ under (a) Severe attacks with $P_I = 0.1$, (b) Moderate attacks with $P_I = 0.1$, (c) Light attacks with $P_I = 0.1$, (d) Severe attacks with $P_I = 0.1$, (e) Moderate attacks with $P_I = 0.5$, (f) Light attacks with $P_I = 0.5$, (g) Severe attacks with $P_I = 0.9$, (h) Moderate attacks with $P_I = 0.9$, and (i) Light attacks with $P_I = 0.9$.

This is because the chances of finding channels with lower rates is higher than that of higher rates, and thus more CRIoT devices can be served.

### B. Testbed Results

To test the efficiency of the BMRJA-MAC protocol in a realistic environment, and to validate our simulation results, we conducted a testbed implementation. For the purpose of experimentation, the FIT IoT-LAB testbed situated in Grenoble, France, is used [28]. FIT IoT-LAB belongs to OneLab consortium and is a multi-user open-source large-scale collection of wireless IoT testbeds providing over 2500 sensor nodes across six different locations in France. The utilized M3 nodes comply with the low-rate IEEE 802.15.4 standard through their radio modules (AT86RF231 radio chip). The nodes are built using ARM Cortex M3 micro-controllers and run using 3.7 V

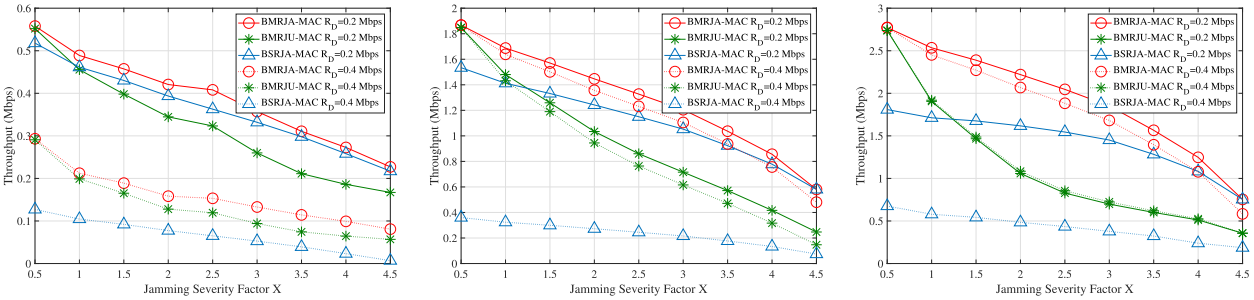



Fig. 6. Testbed throughput performance *vs.* jamming severity for two $R_D$ at $N = 5$ and $M = 10$ given (a) Low $P_I$ (High PU activity), (b) Moderate $P_I$ (Moderate PU activity), and (c) High $P_I$ (Low PU activity).

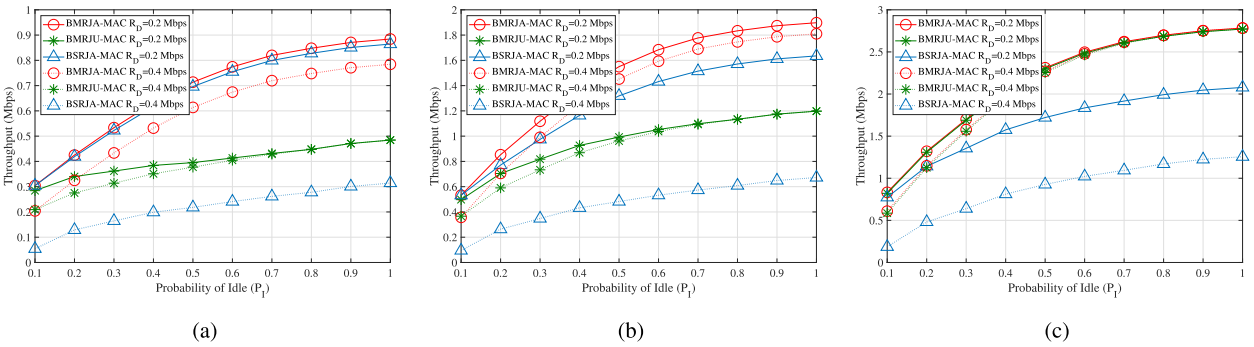



Fig. 7. Testbed throughput *vs.* $P_I$ for $N = 5$ and $M = 10$ under (a) Severe attacks, (b) Moderate attacks, and (c) Light attacks.

Lithium polymer batteries. According to the IEEE 802.15.4 standard, which mandates both the physical and MAC layers, the communication range is 10m to 100m deploying sixteen frequencies around the 2.4 GHz range with a maximum frame size of 127 bytes. One hundred M3 nodes are reserved; they are deployed uniformly as two parallel lines, forming a linear topology, and are fixed on raised floors under the tiles. There are a number of supported operating systems by the M3 nodes (*e.g.* RIOT, Contiki, and FreeRTOS). Our implementation is conducted using FreeRTOS. For the implementation, a custom firmware was generated using libraries created by the manufacturer of the M3 node, HiKoB. Two firmwares were created, one for the nodes acting as CR devices and another for the nodes acting as jammers. The CR device's firmware adopted the FreeRTOS-based CSMA/CA MAC and perform channel condition assessment at the beginning of each transmission. On the other hand, for obtaining the results of the linear program, we used the MATLAB linprog solver. Then, based on the gathered information and user set of parameters (*e.g* delay and throughput requirements), the algorithm was performed on the nodes and the channels were selected. The nodes try to send their packets over the assigned channels, and are allowed to retransmit the packets (when damaged by the jammer) as long as the delay threshold is not exceeded.

The transmission power of each device is 1 dBm and the nodes are chosen randomly at the beginning of each experiment. We consider the same average idle and jamming intervals used in the simulation. Each CR transmission occurs between two randomly selected M3 nodes sending 1000 packets of length 96 bytes each. The nodes are equipped with various sensors including; pressure and light, as well as a gyrometer and an accelerometer. These sensors were forcefully initialized first prior to each run, causing the throughput to be affected by the software processing overhead. Figure 6 illustrates throughput performance with different jamming severity factor values using $R_D = 0.2$, 0.4 Mbps. As can be observed, the behaviour is consistent with the throughput performance provided in Fig. 4 with the main difference of the rate which is restricted by the IEEE 802.15.4 standard. After extensive experimentation, it was discerned that even with no presence of a jammer, network throughput of a single link (*i.e.* single-channel single-CRIoT pair) fairly exceeded 200 Kbps. Figure 7 is also consistent with the simulation results in Fig. 2 showing that our BMRJA-MAC algorithm consistently outperformed the other two protocols.

## VII. Conclusion

This paper proposed a protocol for secure channel assignment in CRIoT networks with delay-critical transmissions under reactive jamming attacks, referred to as BMRJA-MAC. The main key objective of this protocol is to increase the number of CRIoT transmissions that can be simultaneously served in order to enhance network throughput. This protocol employs batching, in which multiple CRIoT devices can simultaneously transmit over multiple channels. Simulation results showed that BMRJA-MAC improved throughput performance compared to other existing protocols under different jamming severity levels, rate demands, and idle probability conditions Specifically, under severe jamming and low PU activities, BMRJA-MAC achieved up to 80% throughput enhancement

over the compared with protocols. Furthermore, the results were validated through testbed implementation using the large-scale FIT IoT-LAB testbed, demonstrating inline results with the simulation analysis.

## REFERENCES


[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[2] J. Wang, Y. Liu, S. Niu, and H. Song, "5G-enabled optimal bi-throughput for UAS swarm networking," in *Proc. Int. Conf. Space-Air-Ground Comput. (SAGC)*, Dec. 2020, pp. 43–48.

[3] J. Wang, Y. Liu, S. Niu, and H. Song, "Reinforcement learning optimized throughput for 5G enhanced swarm UAS networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.

[4] J. Wang, Y. Liu, S. Niu, and H. Song, "Integration of software defined radios and software defined networking towards reinforcement learning enabled unmanned aerial vehicle networks," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Nov. 2019, pp. 44–49.

[5] J. Wang, Y. Liu, S. Niu, and H. Song, "Extensive throughput enhancement for 5G-enabled UAV swarm networking," *IEEE J. Miniaturization Air Space Syst.*, vol. 2, no. 4, pp. 199–208, Dec. 2021.

[6] J. Wang, Y. Liu, S. Niu, and H. Song, "Beamforming-constrained swarm UAS networking routing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2897–2908, Nov. 2020.

[7] J. Wang, Y. Liu, S. Niu, and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Comput. Commun.*, vol. 165, pp. 131–140, Jan. 2021.

[8] J. Wang, Y. Liu, S. Niu, H. Song, W. Jing, and J. Yuan, "Blockchain enabled verification for cellular-connected unmanned aircraft system networking," *Future Gener. Comput. Syst.*, vol. 123, pp. 233–244, Oct. 2021.

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

[10] Y. Liu *et al.*, "Zero-bias deep learning for accurate identification of Internet-of-Things (IoT) devices," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2627–2634, Feb. 2021.

[11] 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. 4829–4842, Dec. 2018.

[12] Y. T. Hou, Y. Shi, and H. D. Sherali, "Spectrum sharing for multi-hop networking with cognitive radios," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 146–155, Jan. 2008.

[13] O. Fambon *et al.*, "FIT IoT-LAB tutorial: Hands-on practice with a very large scale testbed tool for the Internet of Things," in *Proc. UbiMob2014, 10èmes Journées Francophones Mobilité et Ubiquité*, Jun. 2014, pp. 1–5.

[14] M. Yousefvand, N. Ansari, and S. Khorsandi, "Maximizing network capacity of cognitive radio networks by capacity-aware spectrum allocation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5058–5067, Sep. 2015.

[15] C. Chang, S. Wang, and Y. Liu, "A jamming-resistant channel hopping scheme for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6712–6725, Oct. 2017.

[16] B. R. Deepak, P. S. Bharathi, and D. Kumar, "Radio frequency anti-jamming capability improvement for cognitive radio networks: An evolutionary game theoretical approach," in *Proc. 4th Int. Conf. Signal Process., Commun. Netw. (ICSCN)*, Mar. 2017, pp. 1–6.

[17] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2017, pp. 2087–2091.

[18] K. Elangovan and S. Subashini, "Particle bee optimized convolution neural network for managing security using cross-layer design in cognitive radio network," *J. Ambient Intell. Hum. Comput.*, vol. 97, pp. 1–9, Aug. 2018.

[19] P. Zhou, Q. Wang, W. Wang, Y. Hu, and D. Wu, "Near-optimal and practical jamming-resistant energy-efficient cognitive radio communications," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2807–2822, Nov. 2017.

[20] M. Al-Quraan, "Securing delay-sensitive cognitive radio Internet-of-Things communications under jamming attacks: Parallel transmission and batching perspective," M.S thesis, Dept. Telecommun. Eng., Arabic Digit. Library-Yarmouk Univ., Irbid, Jordan, 2020.

[21] 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, 2nd Quart., 2017.

[22] 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, 4th Quart. 2009.

[23] 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.

[24] E. Arikan, "Some complexity results about packet radio networks (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 4, pp. 681–685, Jul. 1984.

[25] L. Liberti, "A useful characterization of the feasible region of binary linear programs," in *Proc. 6th Cologne Twente Workshop Graphs Combinat. Optim.* Enschede, The Netherlands: Univ. Twente, May 2007, pp. 103–107.

[26] L. Wolsey, *Integer Programming*. Hoboken, NJ, USA: Wiley, 1998.

[27] A. Muqattash and M. Krunz, "POWMAC: A single-channel power-control protocol for throughput enhancement in wireless ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 5, pp. 1067–1084, May 2005.

[28] C. Adjih *et al.*, "FIT IoT-LAB: A large scale open experimental IoT testbed," in *Proc. IEEE World Forum Internet Things (IEEE WF-IoT)*, Milan, Italy, Dec. 2015, pp. 459–464.



**Haythem A. Bany Salameh** (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Arizona in 2009. He is currently a Professor of Telecommunication Engineering with Al Ain University, Al Ain, United Arab Emirates, and Yarmouk University, Jordan. His research interests include wireless communications technology, the IoT security, and computer networking.

**Monette H. Khadr** (Graduate Student Member, IEEE) received the Ph.D. degree in electrical and computer engineering, University at Albany–SUNY, Albany, in 2021. Her research interests include machine learning-based optimization of wireless systems, heterogeneous wireless networks, spectrum management, and physical layer security.

**Mohammad Al-Quraan** (Student Member, IEEE) received the M.Sc. degree in wireless telecommunications engineering from Yarmouk University, Jordan, in 2019. He is currently pursuing the Ph.D. degree with the School of Engineering, University of Glasgow. His research interests include wireless communications, AI, ML, Beyond 5G, 6G networking.

**Moussa Ayyash** (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering. He is currently a Professor at Chicago State University, Chicago, IL, USA. His current research interests span digital and data communication areas, wireless networking, visible light communications, network security, and ML.

**Hany Elgala** (Member, IEEE) received the Ph.D. degree from Jacobs University, Germany, in 2010. He is currently an Assistant Professor with the Electrical and Computer Engineering Department, University at Albany–State University of New York, Albany, USA. His research interests include wireless networks, digital signal processing, and embedded systems.

**Sufyan Almajali** (Member, IEEE) received the Ph.D. degree in computer science from the Illinois Institute of Technology, Chicago, USA. He is an Associate Professor at Princess Sumaya University for Technology, Jordan. His research interests include the IoT security, edge computing, and network security.