2020

A secure and energy-aware approach for cognitive radio communications

Haitham Khaled
Edith Cowan University

Iftekhar Ahmad
Edith Cowan University

Daryoush Habibi
Edith Cowan University

Quoc Viet Phung
Edith Cowan University

10.1109/OJCOMS.2020.3009241
Khaled, H., Ahmad, I., Habibi, D., & Phung, Q. V. (2020). A secure and energy-aware approach for cognitive radio communications. *IEEE Open Journal of the Communications Society, 1*, 900-915. https://doi.org/10.1109/OJCOMS.2020.3009241

Received 16 June 2020; revised 10 July 2020; accepted 10 July 2020. Date of publication 14 July 2020; date of current version 28 July 2020.
Digital Object Identifier 10.1109/OJCOMS.2020.3009241

A Secure and Energy-Aware Approach For Cognitive Radio Communications

HAITHAM KHALED (Student Member, IEEE), IFTEKHAR AHMAD (Member, IEEE), DARYOUSH HABIBI (Senior Member, IEEE), AND QUOC VIET PHUNG (Member, IEEE)
School of Engineering, Edith Cowan University, Perth, WA 6027, Australia
CORRESPONDING AUTHOR: H. KHALED (e-mail: hkhaled@our.ecu.edu.au)

ABSTRACT The cognitive radio (CR) technique has revealed a novel way of utilizing the precious radio spectrum via allowing unlicensed users to opportunistically access unutilized licensed bands. Using such a technique enables agile and flexible access to the radio spectrum and can resolve the spectrum-scarcity problem and maximize spectrum efficiency. However, two major impediments have been limiting the widespread adoption of cognitive radio technology. The software-defined radio technology, which is the enabling technology for the CR technique, is power-hungry and this raises a major concern for battery-constrained devices such as smart phones and laptops. Secondly, the opportunistic and open nature of the CR can lead to major security concerns about the data being sent and how safe it is. In this paper, we introduce an energy-and-security-aware CR-based communication approach that alleviates the power consumption of the CR technique and enhances its security measures according to the confidentiality level of the data being sent. Furthermore, the proposed approach takes into account user-related factors, such as the user's battery level and user's data type, and network-related factors, such as the number of unutilized bands and vulnerability level and then models the research question as a constrained optimization problem. Considering the time complexity of the optimum solution, we also propose a heuristic solution. We examine the proposed solution against existing solutions, and our obtained results show that the proposed approach can save energy consumption up to 18%, increase user throughput up to 20%, and achieve better spectrum utilization, up to 98%. Our proposed admission approach has the potential to open a new research direction towards safer and greener cognitive radio techniques.

INDEX TERMS Cognitive radio, next generation wireless networks, green communications, cognitive radio security issues, software defined radio.

I. INTRODUCTION

FUELED by the widespread adoption of wireless-enabled devices and their data-hungry applications, mobile data traffic has dramatically increased in recent years. Mobile data traffic is anticipated to witness another seven-fold growth, reaching 86% of global data traffic by 2022 [1]. Additionally, owing to the random nature of user demands and mobility, mobile data traffic has become more random, diverse, and unevenly distributed across time and space [2]. This trend of growth has not only forced mobile-network operators to intensify their power consumption, but also to add more spectrum to expand their network capacity to accommodate users' ever-increasing demands. Nevertheless, licensed-spectrum is scarce and imposes extra operational costs on network operators. Augmented by scarce spectral resources, these drastic challenges result in a dilemma for mobile-network operators in managing and maintaining network capacity, user demands, and quality of experience [3].

Cognitive radio (CR) is considered one of the promising technologies to tackle the above-mentioned challenges [4]. In CR, a software-defined radio (SDR)-enabled mobile device can dynamically adapt and reconfigure its transmission parameters according to the surrounding spectral-environment [5]. This allows CR-enabled devices, commonly known as secondary users (SUs), to dynamically access unutilized frequency-bands in the surrounding networks

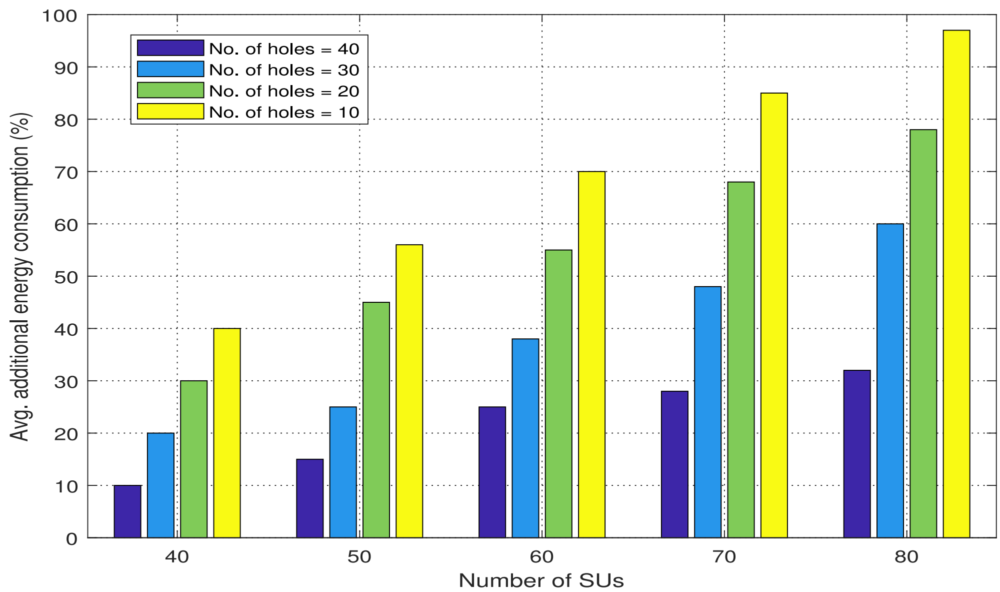

FIGURE 1. The influence of increasing the number of contending SUs on total consumed power [13].

without interfering with those networks' original incumbents, termed as primary users (PUs) [6]. Accordingly, CR can help mobile network operators to expand their usable spectrum at a comparatively low cost to meet diverse, random and exploding mobile traffic demands [7].

In this regard, due to its ubiquitous accessibility and reduced operational cost, the unlicensed spectrum is predicted to play a key role in providing low-cost spectrum access and augmenting bandwidth and capacity available for mobile operators to utilize [8]. Consequently, this can help users to gain a better quality of experience (QoE) and operators to reduce their operational expenditure (OPEX). Accordingly, the mobile communication industry has witnessed a gradual convergence between licensed and unlicensed spectrum technologies recently [9]. The increasing interest in unlicensed spectrum by mobile communication service providers is apparent in the introduction of solutions that leverage mobile technologies in the unlicensed band (e.g., 5 GHz) along with the mobile licensed spectrum as shown in [10].

While the cognitive radio technique, along with the unlicensed spectrum, can help both users and network operators to meet explosive traffic demands, its cognition procedures, such as scanning for unutilized bands and switching between them, are particularly power-intensive [11]. In other words, its cost in terms of power consumption is higher than the traditional communication technique [12]. In CR, secondary users contend for the unutilized/free frequency bands within a spectrum. Subsequently, as shown in Fig. 1 [13], more contending SUs lead to higher average power consumption [14]–[16]. SDR technology heavily relies on field-programmable gate arrays (FPGAs) which consume more power than application specific integrated circuit (ASIC) chips that are used in traditional communication devices [17]. All these power-related factors contribute towards the higher cost of the CR technique and represent an apprehension for battery-constrained devices that rely heavily on their limited battery to operate.

Information security is also a concern in CR. Owing to the opportunistic and relatively open nature of the CR, CR-enabled devices are susceptible to security attacks targeting the medium access (MAC) or physical layer while accessing different networks than their own host network [18]. For instance, eavesdropping, spoofing, jamming, and wire-tap [19], [20] are major concerns. CR-enabled devices are prone to other security attacks that misuse their cognitive characteristics. Examples include spectrum sensing data falsification (SSDF) attacks and primary user emulation attack (PUEA) [21]. Moreover, as CR-enabled devices are based on SDR, these devices are vulnerable to software-based threats [22]. Accordingly, these security concerns can be considered as an additional cost for using the CR technique.

Both power and security-related costs can submerge the benefits offered by the cognitive radio communication paradigm. If not adequately managed, power-related costs can cause a rapid battery depletion for battery-constrained portable devices. This can result in less up-time for these devices. Additionally, security-related costs can cause a confidentiality/privacy breach of users' sensitive data. Accordingly, permitting all CR-enabled users (i.e., SUs) to participate and contend for unutilized/idle spectrum bands in any network, irrespective of their traffic types, traffic size, and the battery level is not a sound approach.

In this paper, we introduce an energy and security-aware approach that maximizes the benefits of CR-enabled users. The main idea is based on restricting the CR participation process to SUs who would achieve the highest benefit in return for their extra power consumption and security risks. By adopting such an approach, the number of SUs who would contend for unutilized/idle bands is kept at a reasonable level to maintain high benefits for all participants.

The main contribution of this work can be summarised as follows:

- We introduce an energy and security-aware CR-based communication approach that maximizes user benefits and minimizes power costs.
- We formulate the research challenge as a constrained optimization problem and provide a solution to the optimization problem.
- Due to the computational complexity of the optimization problem, we propose a heuristic solution that offers promising results.

The rest of the paper is organized as follows: The next section summarizes prior related works and discusses how this research paper covers gaps in prior research works. Additionally, the section will present the problem statement that this research work is trying to solve. In Section III, we illustrate and explain our system model and the different parameters including network model, communication model, benefit mode, power model, and vulnerability model. Additionally, in this section, we introduce and explain our algorithm-based admission control mechanism and our proposed heuristic. Section IV displays our obtained simulation results and gives a detailed discussion about these results and findings. Section V introduces the concluding remarks.

II. RELATED WORKS AND PROBLEM STATEMENT

A. RELATED WORKS

Recently, cognitive radio has emerged in numerous research papers as a promising technology to solve the spectrum inefficiency/scarcity problem. For instance, in [23], secondary users have been categorized by the authors based on their required quality of service, and by utilizing an auction-based model, where the authors increased the spectrum efficiency of their network. The authors in [24], presented multiple cooperation policies between SUs and primary users (PUs). These policies are based on Markov decisions and aimed to reduce SUs' blocking probability for better throughput and spectrum efficiency. In [25], three sub-carriers selection approaches were introduced by the authors to boost SUs' signal to interference and noise ratio (SINR) to maximize their data throughput.

In [26], the authors have proposed techniques and algorithms to predict the idle bands of the spectrum. These techniques and algorithms are utilized by SUs to access the idle frequency bands and transmit the data. Authors in [27] have presented a repeated-game-based strategy, that allows CR-enabled devices to increase their throughput and decrease the probability of collisions with other CR-enabled devices that are contending on the idle bands of a spectrum. The authors in [28] have introduced a novel cooperative spectrum-sensing technique, based on an optimal energy-detection technique and can reduce the probability of detecting fake idle frequency bands in a spectrum. In [29], the authors have presented a comprehensive review for main and indispensable spectrum-sensing techniques and media access strategies used in cognitive radio.

While the above-mentioned studies have been useful in managing the cooperation between SUs and PUs, predicting idle spectrum bands, boosting SUs' achievable throughput, increasing SINR and spectrum efficiency, and decreasing blocking probabilities and fake PUs detection, none of these studies have considered the extra power required to be consumed during the cognitive radio procedures and the affordability of the CR-enabled devices for such extra power. For battery-constrained devices, such as laptops and smart phones, this extra power can easily overwhelm the benefits achieved by their proposed approaches. Accordingly, the power affordability of a CR-enabled device, for such a paradigm in communication, represents a significant influence on CR reliability.

Owing to the wireless nature of the CR, it is susceptible to various threats and attacks. Hence, several researchers worked in securing the CR paradigm. For instance, authors in [30], listed several common security attacks/threats to CR physical layer and proposed some countermeasures that can be utilized to protect CR users. In [31], the authors presented a list of current network layer attacks and their countermeasures. Authors in [32], have presented a secured transmission approach that can be used in a CR-based network. Reference [33] provided a novel approach to identify and isolate a selfish attacker in a CR-based network. The authors in [22] comprehensively presented most of the security attacks/threats in the CR-based networks and the detection techniques that can be utilized to detect these attacks. In [21], the authors have defined the byzantine attack, which is one of the common attacks in CR-based networks, and have presented an overview of the existing research studies that aim to defend against this attack.

While the previously-mentioned studies and surveys are advantageous in detecting and defending any security attack/threat in CR-based communication paradigm, none of them have considered the transmitted data sensitivity and the extra power requirements to adhere to these security techniques and countermeasures. In other words, most of the previously-mentioned works had the assumption that all CR-enabled devices have very high confidential data, and hence sensitive, to send and unlimited power resource that allows these devices to implement and adhere to the security countermeasures. For our normal daily use of battery-constrained devices, this assumption is not always accurate. Hence, for low-battery CR-enabled devices with insensitive data to send, these security measures and techniques could consume extra power from its precious limited power resource and add more overheads for unapparent reasonable cause. This can also overwhelm the benefits offered by these techniques. Accordingly, data sensitivity and power consumption affordability should be considered before applying these countermeasures to avoid overwhelming CR benefits.

TABLE 1. Key differences of our proposed mechanism.

Parameters Considered	Authors in [24]–[29]	Authors in [21], [22], [30]–[33]	Authors in [34]–[37]	Proposed mechanism
Number of SUs	-	-	-	✓
Traffic size	✓	-	✓	✓
Traffic type	-	✓	-	✓
Total Power consumption	✓	-	✓	✓
Total throughput Or blocking probability	✓	✓	-	✓
Safe transmission	-	✓	-	✓
SU's battery-level	-	-	-	✓

Energy efficiency in CR has also been covered widely in the literature. For instance, [34] has presented an energy-harvesting-based CR technique that trade-off both energy efficiency and spectrum efficiency to achieve high benefit from CR technology. Leveraging CR, the authors in [35] presented a cooperation mechanism between secondary base stations (SBSs) and primary BSs (PBSs) to reduce power consumption of both BSs and to increase spectrum efficiency. The authors in [36] presented an overview of various energy-efficient techniques that are used in spectrum sensing to locate idle frequency bands in a spectrum. In [37], the authors have utilized green-energy to the CR to boost the energy efficiency and reduce the overall power consumption.

While the above-mentioned research studies (i.e., [34]–[37]) have presented useful mechanisms and techniques to increase the energy efficiency of CR processes and networks, these studies have not considered the security aspect in their communication method, and assumed that all CR-enabled devices (i.e., SUs) are equipped with unlimited power resource, where it is affordable for all of them to participate in the CR process. However, this consideration is not accurate as wireless communication networks serve different mobile users with different data traffic needs, limited-power resources, and different types of traffic (i.e., confidential or not). Accordingly, the affordability is different from one user to another.

Most of all the above-mentioned research studies have presumed that all SUs are consistently ready to utilize the CR technique and all benefit from it. However, with considering the extra power consumption and the extra security risks associated with the CR technique, such an assumption is not always accurate and not all SUs would benefit equally from CR. Hence, unlike the above-mentioned studies, in this paper, we present a novel CR approach that considers the extra power consumption, the sensitivity of data being sent, and network vulnerability before allowing users to use their CR abilities.

Unlike the traditional approach that is utilized in the previous studies, our proposed approach shortlists the participating CR-enabled devices based on their gained benefits from the CR process. Accordingly, only devices that benefit the most from the CR process will be allowed to participate. By removing CR-enabled devices that do not benefit from the CR process, the number of users contending for idle frequency bands in the spectrum will be reduced. Thus, owing to the less contention, the power consumed by the SUs in the list will be reduced as previously shown in Fig. 1. In this work, the benefit is quantified in terms of CR-enabled device's battery-level (i.e., affordability), type of traffic (i.e., confidentiality), size of traffic, and total power consumption.

Table 1 summarizes the key differences between our proposed mechanism and the other mechanisms covered in the related works section. As shown in Table 1, most research studies in the literature have focused either on reducing the total power consumption or increasing the security level of the CR communication paradigm. At this point, Table 1 summarizes the parameters considered in these research studies to calculate the benefit gained by their cognitive radio paradigm. To the best of our knowledge, our proposed mechanism is the first to consider both reducing total power consumption and increasing the security of the CR-based transmission to increase the overall benefit of CR-enabled SUs while considering all the parameters listed in Table 1. Additionally, except for our proposed mechanism, most of the above-mentioned studies have not considered the SU's battery-level or number of SUs contending on the free/idle bands in a spectrum in their benefit.

B. PROBLEM STATEMENT

For battery-constrained devices such as laptops and smart phones [11], [12], [16], the costs associated with the additional power consumption and security risks of the cognitive radio technique can be overwhelming. For instance, for a CR-enabled user (i.e., a secondary user) whose device's battery level is low and has non-critical data to send, the magnitude of the benefit that the CR technique offers can be easily overwhelmed by the cost associated with rapid battery depletion due to CR's power-hungry procedures. The

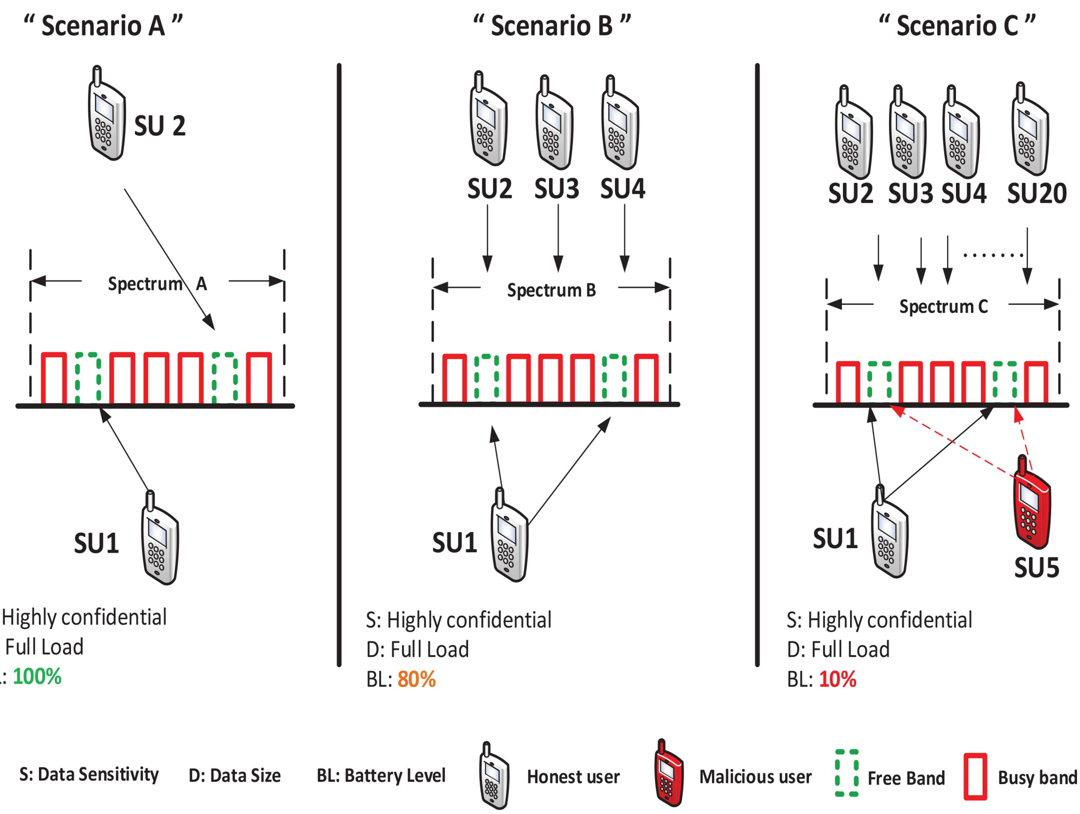

FIGURE 2. Different Cognitive Radio Scenarios.

same thing applies when a user has critical data to send and the CR technique picks a network that is vulnerable to security attacks.

Given the above-mentioned power and security related costs associated with the CR technique, not all SUs would benefit equally from the CR technique. Additionally, as shown in Fig. 1 and in literature [14]–[16], the more SUs compete for free/idle bands, the more power they would all consume to send their data. Consequently, the research question becomes- how to select/short-list secondary users to participate in the cognitive radio process so that their overall benefits can be maximized and corresponding costs in relation to power and security remain low. In this paper, we introduce a cognitive radio communication approach that addresses this research challenge.

III. PROPOSED SECURE-GREEN COGNITIVE RADIO MODEL

In this section, we introduce a description of our energy and security-aware cognitive radio system model shown in Fig. 3. This description covers the network model, communication model, benefit model, power model, and the vulnerability model.

The main aim of this work is to maximize the total benefit, in terms of total throughput of all users, while minimizing total costs, in terms of users' power consumption. To accomplish this, the number of SUs contending for free/idle bands in a spectrum should be restricted since increasing the amount/number of contention leads to higher average power consumption. The shortlisted SUs should be carefully/optimally chosen in order to maximize the benefit and minimize power costs without compromising data confidentiality.

To illustrate, even further, take an example of the secondary user 1 (SU1) in the three scenarios illustrated in Fig. 2. In all scenarios, SU1 has a full load of data (D), a very sensitive/confidential type of data (S), and the same number of free bands. However, the differences between the three scenarios are the battery level (BL) of SU1, the number of competing SUs, and the vulnerability level of the accessed spectrum. In scenario (a), SU1 is only competing with another single SU and SU1 has a decent battery level. Accordingly, for SU1, the cost required for the CR approach is considerably low because of the low contention level and the high level of battery affordability. Hence, in such a scenario, allowing SU1 to utilize the free bands, via the CR technique, can translate into higher benefits in terms of higher data rate and throughput.

Compared to scenario (a), the number of competing SUs in scenario (b) is much higher and the SU1's battery level is even lower. Hence, for the SU1 and compared to scenario (a), the required cost to participate in the CR technique is higher and the amount of benefit, in terms of higher data rate and throughput, is less than scenario (a). For scenario (c), SU1 has a critical battery level, a higher number of SUs competing on free bands, and some of these SUs are

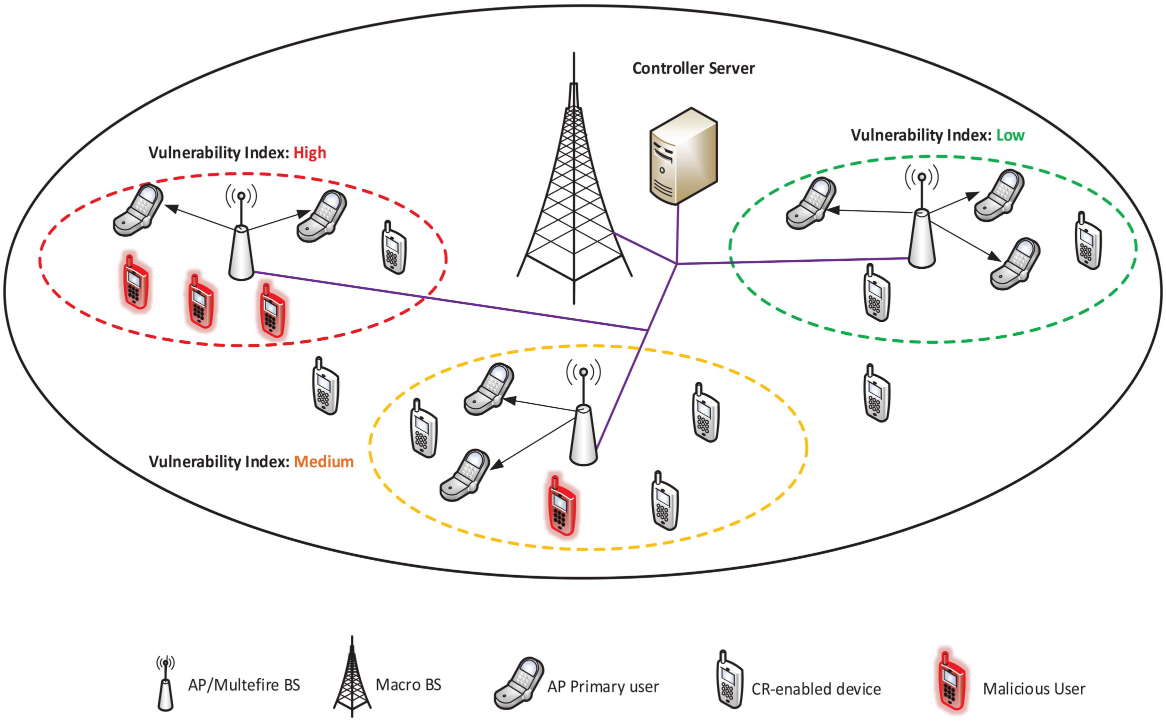

FIGURE 3. System model.

malicious users representing a high vulnerability level. Thus, compared to scenarios (a) and (b), SU1's cost is significantly higher in this scenario. Additionally, the amount of benefit is much less and is very vulnerable.

Based on the above-mentioned scenarios, the CR technique is not for everyone and not for every situation. Hence, our proposed approach restricts the CR techniques in communication to shortlisted SUs. These chosen SUs are optimally chosen to maximize the total benefits of the shortlisted SUs and minimize their costs.

A. NETWORK MODEL

The network model of our proposed approach is illustrated in Fig. 3. The system model is comprised of a macro base station, multiple access points with their primary users connected to them, a controller sever, and several end-users that are equipped with cognitive-radio-enabled (CR-enabled) devices and primarily connected to the macro BS (MBS). In our model, all the access points (APs) are operating in the unlicensed band (i.e., 5 GHz). However, some of these APs use the IEEE 802.11 standard (WiFi technology) [38] which is the main incumbent technology in the unlicensed band [39], [40] and the rest of these APs are utilizing MultiFire technology which is a standalone Long-Term Evolution (LTE) in the unlicensed band. The technical specifications of this radio access technique, named MultiFire, were finalized and published in mid of 2017 [41], [42].

Furthermore, as shown in Fig. 3, the controller sever is connected to the APs and the MBS. It regularly gathers information from the APs and MBS about their free/used bands, traffic loads, the number of connected users, and connection costs. Additionally, it collects from the users, through the MBS, their battery levels, data rate requirements, and confidentiality requirements. Subsequently, according to the obtained information and the APs' vulnerability indexes that the server has, the controller server selects/short-lists which users should participate in the CR procedures and which AP to be associated with. Consequently, the controller server informs the short-listed users, through the MBS, about the most suitable AP for them and instructs them to use their CR capabilities to access it.

Such a network model can practically exist/utilized where a mobile operator has a MBS that covers a users-dense area, such as a city business district (CBD) that has a mall, a train station, a library, and various multi-storey office buildings. This area already has various types of APs, from a security perspective, that also managed by the same mobile operator. The types of APs range from open access AP, similar to the WiFi APs in malls nowadays, through password-protected APs, to MultiFire APs that utilize high-security measures to protect their users.

Owing to the high number of users being served, increasing users' demand for extra data, and the limited licensed band, the MBS cannot meet all the users' demands. Hence, the MBS, with the controller server's support, select/short-list some of its connected users to access nearby APs by utilizing their CR abilities.

The process of pairing users with APs should consider the users' data confidentiality and APs vulnerability level and its impact on users' data. Additionally, it should consider the existing load if the APs, because, as previously explained, more users translates to higher power consumption, which is not appreciated for battery constrained devices. Accordingly, the users are shortlisted so that their overall CR benefits can be maximized and corresponding costs in relation to power and security remain low.

The users set is denoted as $\mathcal{J} = \{1, 2, 3, \ldots, j, \ldots, N\}$. In our system model, the users' CR-enabled devices are all portable and wireless-enabled. The battery level of the jth user is represented by B_j where $0 < B_j \leq 1$ and 0 represents an empty battery and 1 means a fully charged battery. For user j, the data size and confidentiality are expressed as D_j and μ_j, respectively, and $0 \leq \mu_j \leq 1$ where 0 means the data is not confidential and can be shared and 1 means it is strictly confidential. Additionally, in our system model, the users' data sizes and confidentiality are not related or dependant on each other.

It worth highlighting that the users are utilizing the overlay CR access strategy, where SUs perform spectrum-sensing and send the data during the absence of the primary occupant/user. When the PU is active gain, the SU needs to refrain from using this band and find another band [6], [43], [44]. Such an access strategy requires no cooperation with the PU and offers flexible control and higher data rate compared to the underlay access strategy, in which both SU and PU can use the same band at the same time, however, the interference caused by the SU must not exceed a tolerable threshold [45], which requires cooperation with the PU and high level of complexity to maintain the interference level with PU under a certain level [44], [45].

The APs' set is denoted as $\mathcal{I} = \{1, 2, 3, \ldots, i, \ldots, M\}$ and each AP has a number of free/idle bands that secondary users can utilize to send their data denoted by F_i and with a bandwidth of W_i. These access points are offering these bands for CR access for a monetary reward of C_{ij}.

B. SECURITY AND RISK FACTOR

The probability of a security breach (sniffing, spoofing, eavesdropping, …, etc) to occur at AP i is presented by the vulnerability index δ_i where $0 < \delta_i \leq 1$. 0 represents a 100% safe/non-vulnerable AP, which does not exist, and 1 represents an extremely vulnerable AP. The vulnerability here is presented by the probability of having malicious user/users within the AP coverage area that can make the AP prone to a security breach (sniffing, spoofing, eavesdropping, etc.) [46]. Hence, the risk factor that is recognized by user j at AP i can be expressed as:

$$\zeta_{ij} = \frac{\mu_j}{\delta_i} \tag{1}$$

accordingly, when user j has high confidential data and is accessing a very vulnerable AP i, the user will recognize a high value of ζ_{ij}, high risk factor, and vice versa.

In our system model, since the MBS works only in the licensed band, serves only licensed users, authenticates its users by their valid subscriber identification module (SIM), and utilizes various encryption keys to secure its communication with its users [47], then its vulnerability index is the lowest. Subsequently, although the AP with MultiFire technology authenticates its users via their SIM cards, it works completely in the unlicensed band, which is a band that is accessible by an extremely wide range of users and technologies. This makes it more vulnerable for security attacks than the MBS. Hence, the AP with MultiFire technology has a slightly higher vulnerability level than MBS [42].

For the APs that use the IEEE 802.11 standard (WiFi technology) [38], they all work in the unlicensed band and they all allow any WiFi-enabled user, irrespective of their intention, to get connected. Some of these APs are password-protected where only users who know the predefined password can be granted the access, and the rest are open (i.e., not password-protected) for the public use, such as the APs in train stations, airports, and malls.

Since the WiFi APs utilize a password-based security measure to control the users' accessibility, the WiFi APs' vulnerability level is much higher than the MultiFire AP and MBS. The reason for this is, as previously mentioned, the MultiFire AP and MBS utilize multiple extensive security measures including a hardware-based security measure (i.e., SIM cards) and extensive encryption to authenticate and secure their communications with their users [47]. However, in the case of WiFi APs, a limited software-based security measure (i.e., password) is utilized, which makes them much more prone to security breaches [40].

Accordingly, on our system model, the vulnerability index of the password-protected WiFi AP is much higher than MultiFire AP and MBS, and the vulnerability index of the public WiFi APs is even higher.

In order to quantify the suitability of a CR-enabled device/user j to access AP i with its battery status B_j, with a risk factor ζ_{ij}, we introduce another factor named the suitability factor that can be calculated as:

$$\varepsilon_{ij} = \frac{B_j}{\zeta_{ij}} \tag{2}$$

thus, for a device with a battery level B_j to be able to use its CR ability, he needs to pick an AP with low ζ_{ij} to increase its suitability for the CR process.

C. COMMUNICATION MODEL

We assume users' positions are fixed/static during an iteration. However, their positions may change in the next one. We represent the transmission power of AP i as P_i and the channel gain from AP i to user j as g_{ij}, which typically includes shadowing, path loss, antenna gain, and reflects the slow fading [48]. Furthermore, we presume the channel gain is calculated at large time scale, compared to the change of the channel, thus fast fading is not considered. Such an assumption has been adopted in previous works such as [35], [48], [49]. The noise power level is denoted as σ^2.

We presume each user encounters a near static interference from interfering APs and other users. Although interference varies according to the network dynamics, it can be well controlled via various frequency domain techniques, time domain techniques, and power control techniques [48]. Accordingly, the interference could be modeled as a static value to simplify the analytical model [48]. Such an approach has been adopted in previous words such as [35], [48], [50].

Accordingly, let $\mathcal{B}_i$ denotes the set of all the interfering APs, whose transmissions interfere with the transmission of i^{th} AP with the user j across all bands. Similarly, $\mathcal{A}_j$ represents the set of all the interfering users whose transmissions interfere with the transmission of j^{th} user with the AP i across all bands. $\mathcal{B}^i_v$ and $\mathcal{A}^j_o$ are the average interference recognized by user j from v^{th} AP and o^{th} user, respectively [51].

Accordingly, the signal to interference plus noise ratio (SINR) of an AP i toward user j can be expressed as;

$$SINR_{ij} = \frac{P_j \cdot g_{ij}}{\sum_{v \in \mathcal{B}_i} \mathcal{B}^i_v + \sum_{o \in \mathcal{A}_j} \mathcal{A}^j_o + \sigma^2} \tag{3}$$

hence, the data rate R_{ij} of user j as AP i can be derived as a logarithmic function according to Shannon theorem as follows;

$$R_{ij} = F_{ij} \cdot W_i \cdot Log(1 + SINR_{ij}) \tag{4}$$

where F_{ij} and W_i represent the number of free/idle bands allocated to user j and the size of each band at ith AP, respectively. It worth highlighting that a user can use multiple bands, if his hardware is capable to do this. This has been used to add more flexibility to our mathematical model.

D. BENEFIT MODEL

To quantify the benefit of user j from using the CR technique to access the idle bands of AP i, we calculate the cost per bit at this AP, C_{ij}, and compare it with the cost per bit at the macro BS, C_m. Hence, the amount of benefit that can be achieved by the user j is the difference between the two prices. Thus, the benefit/saving can be expressed as follows:

$$S_{ij} = R_{ij} \cdot (C_m - C_{ij}) \tag{5}$$

Owing to users' inconsistency of demands and activity patterns, each AP has variable demands and different amounts of available resources to offer during the day (e.g., peak vs off-peak hours). Hence, C_{ij} is not a standard fixed price for all APs, and it changes according to the APs' instantaneous-load level. The price/cost increases when the AP's load increases and vice versa. Such an approach protects the AP from being overwhelmed by the SUs request and being overloaded with SUs.

In our model, a linear pricing model has been adopted, where the AP increases the price/cost of accessibility when the number of SUs associated with it increases and decreases the price when the number of SUs decreases. Hence, the pricing model identifies the price/cost for a service depending on its traffic demands and available supplies. Accordingly, C_{ij} can be expressed as [52]:

$$C_{ij} = a \cdot \eta_{ij} + C_i \tag{6}$$

where C_i denotes the base/standard price of AP i, a represents the slop of the price/demand curve, and η_{ij} denotes the ratio between the number of SUs associated with the AP, including user j and the number of free/idle bands at this AP. Hence, η_{ij} can be calculated as follows:

$$\eta_{ij} = \frac{\hat{N}_{ij}}{F_i} \tag{7}$$

where $\hat{N}_{ij}$ presents the total number of SUs associated to SUs, including user j, and F_i denotes the total number of free/idle bands.

E. POWER MODEL

For the user j, the total power consumed to send data using the CR technique includes the consumed power to scan the spectrum to search for idle bands, to switch between idle bands, and to transmit data through these bands. The power to send data can be expressed as [13], [14]:

$$P^{pkt}_j = P^{tr}_j + \frac{p_k}{1 - p_k} \cdot P^{co}_j + H(p_k) \cdot P^{bck}_j \tag{8}$$

where P^{pkt}_j is the consumed power to send a single packet by user j, P^{tr}_j represents the transmission power for the same user, p_k expresses probability for collision with k contending users, P^{co}_j denotes the power consumed by user j during collision, P^{bck}_j denotes the consumed power at back-off state, and $H(p_k)$ is the number of counted bands before the packet of data is actually sent. It presents the anticipated number of bands that need to be checked for availability before the packet is actually sent. $H(p_k)$ was derived and analyzed in [14], [53] as;

$$H(p_k) = \gamma \cdot \frac{(1 - p_k) - p_k \cdot (2 \cdot p_k)^{\omega}}{1 - 2p_k} - 1 \tag{9}$$

where γ represents the initial back-off contention window size in the AP that can be set by the AP and shared with the users and controller server to be able to process the proposed algorithm. ω represents the number of times that the back-off window can be extended before reaching the maximum.

In this article, we use a scanning technique where the user j scans all the idle bands in AP i first and then selects the one for which the contention is lesser by a pre-determined threshold β. Accordingly, the total scanning power can be formulated as:

$$P^{sc}_{ij} = (F_i - 1) \cdot [P^{scb}_j + P^{sw}_j] + \rho_{ij} \cdot P^{sw}_j \tag{10}$$

where P^{scb}_j is the power consumed to scan a single band by user j. P^{sw}_j is the power consumed to switch between bands. This power is basically consumed by user j to change its SDR-based communication parameters to switch between bands. ρ_{ij} represents the probability that user j at AP i will switch from the existing band to another one and it is expressed as:

$$\rho_{ij} = \sum_{q=1}^{F_i} \varrho_{ij}(1 - \varrho_{ij})^{q-1} \tag{11}$$

where ϱ_{ij} denotes the probability that user j can detect a better band, lesser contention, at AP i. ϱ_{ij} can be derived as [54]:

$$\varrho_{ij} = F_x^i(k_i - \Delta_i) - \beta_j e^{-\beta_j(k_i - \Delta_i)} \tag{12}$$

where $F_x(\cdot)$ represents the cumulative distribution function of contending users at each band. k represents the number of users contending on bands and Δ_i represents the mean number of SUs per idle band at AP i.

Accordingly, the total power consumed by user j to send data using the CR technique P_j^{cr} through AP i can be formulated as:

$$P_{ij}^{cr} = (F_i - 1) \cdot [P_j^{scb} + P_j^{sw}] + \rho \cdot P_j^{sw} + P_{ij}^{tr} \tag{13}$$

where P_{ij}^{tr} is the consumed power by user j while sending data through AP i and can be calculated as:

$$P_{ij}^{tr} = R_{ij} \cdot D_j \cdot P_j^{pkt} \tag{14}$$

where D_j is the amount of data, number of packets, that user j want to send.

F. PROBLEM FORMULATION

As illustrated in our system model in Fig. 3, the MBS covers several APs and various users. Owing to the temporal and spatial dynamics of the mobility of AP users, some APs are underutilized and others are fully-loaded with their native users. Hence, the underutilized APs can offer, for a fee, their unused bands for the CR-enabled users of the MBS to access via the CR technique. However, the vulnerability indexes for these APs are different depending on their protective security mechanisms, and historical data of previous malicious attacks in these APs. Hence, and as shown in Fig. 2, not every CR-enabled user would benefit the most from these APs.

Thus, to optimally exploit the available bands offered by the APs, only the CR-enabled users that benefit the most should be permitted to participate in the CR process in order to access the APs' offered unutilized-bands. In this paper, the benefit for the user j accessing the AP i is quantified as:

$$\lambda_{ij} = X_{ij} \cdot \varepsilon_{ij} \cdot \frac{S_{ij}}{P_{ij}^{cr}} \tag{15}$$

where S_{ij}/P_{ij}^{cr} represents the dollar per unit of additional power required by user j to access AP j via the CR process, ε_{ij} denotes the affordability of the user to access that AP as explained in Section III-B, and X_{ij} is a binary decision variable that takes a value of 1 if the user j is using the unutilized-bands offered by AP i and can be presented as follows:

$$X_{ij} = \begin{cases} 1 & \text{if user } j \text{ is using AP } i \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

Once the MBS quantifies the benefits of all users, it can short list the users that can benefit the most from the CR procedures. This can be formulated mathematically as an optimization problem with the aggregated benefit expressed as follows:

$$Z = \sum_{i=1}^{M} \sum_{j=1}^{N} X_{ij} \cdot \varepsilon_{ij} \cdot \frac{S_{ij}}{P_{ij}^{cr}} \tag{17}$$

Hence, the objective function is derived as :

$$\text{maximize } Z \tag{18}$$

subject to

$$X_{ij} \cdot (C_m - Cij) > 0, \qquad \forall j \in \mathcal{J} \quad \forall i \in \mathcal{I} \tag{19}$$

$$\sum_{i=1}^{M} X_{ij} \leq 1, \qquad \forall j \in \mathcal{J} \tag{20}$$

$$\sum_{j=1}^{N} X_{ij} \cdot R_{ij} \leq R_{max}, \qquad \forall i \in \mathcal{I} \tag{21}$$

$$0 < \sum_{j=1}^{N} X_{ij} \leq 2F_i, \qquad \forall i \in \mathcal{I} \tag{22}$$

$$X_{ij} \cdot SINR_{ij} \geq SINR_{ijmin}, \qquad \forall j \in \mathcal{J} \tag{23}$$

where,

- Eq (19) ensures that only users that can attain monetary benefits are shortlisted.
- Eq (20) makes sure that each user is only accessing the unutilized bands of a single AP.
- Eq (21) ensures that the aggregated data rates of users accessing the AP are bounded by the maximum capacity of the AP.
- Eq (22) to ensure that the maximum number of SUs to be associated to an AP is double the number of free bands at this AP. Such a constraint minimizes the SUs back-off period which results in minimizing the consumed power in the CR process [16].
- Eq (23) ensures that SINR for each user is greater than a predefined threshold $SINR_{ijmin}$ to achieve seamless communication between the AP and the user

Here,

$$X = \begin{pmatrix} X_{1,1} & X_{1,2} & X_{1,3} & \dots & X_{1,M} \\ X_{2,1} & X_{2,2} & X_{2,3} & \dots & X_{2,M} \\ X_{3,1} & X_{3,2} & X_{3,3} & \dots & X_{3,M} \\ \vdots & \vdots & \vdots & \ddots & \\ X_{N,1} & X_{N,2} & X_{N,3} & \dots\dots & X_{N,M} \end{pmatrix} \tag{24}$$

For the above-mentioned integer linear programming problem (ILP), we used IBM CPLEX studio to resolve. The obtained results are demonstrated and discussed in Section IV. However, solving such a problem in the real-time with a large coverage area and a large number of users is a challenging task. Hence, we have proposed the following heuristic.

Algorithm 1 The Cognitive Radio Algorithm

Input: SUs j $\in \mathcal{J}$; battery-level B_j; Data demand D_j;Confidentiality index μ_j
Output: The optimum-list of SUs to achieve maximum benefit
for every time slot $t \in 1, 2, \ldots, T$ **do**,
  for each user demanding APs accessibility via CR **do**
    Calculate λ_{ij} using equation (15).
    Sort N users in descending order
    if $\lambda_{ij} \leq \Lambda$ **then**,
      move the user to φ; Not-suitable-candidates list
    else
      move the user to Γ; suitable-candidates list
    end if
  end for
  Run Algorithm 2
  allow users to access APs according to Π
end for

Algorithm 2 The BC-Algorithm

Step1: For users Γ do initial assignment
Step2: Set F=0; find $j = argmin_{j \in J} Z_{ij}$; $(\hat{\Pi}, F) = new\_AP\_search\ (j^*, \Pi)$;
if $F == 1$ **then**
  $\Pi = \hat{\Pi}$;
  Jump to step 2;
else
  Step 3:
  if $\{j$ can access other APs$\}$ **then**
    Find $Y_b = \{j | \Pi_{j,b} = 1, \Pi_{j,b} = 1, j \neq i, j \in \mathcal{J}\}$;
    for $j = 1 : |Y_b|$ **do**
      Remove the markers;
      $(\hat{\Pi}, F) = new\_AP\_search\ (j^*, \Pi)$;
      if $F == 1$ **then**
        $\Pi = \hat{\Pi}$ and terminate;
      end if
    end for
    if $F == 1$ **then**
      Jump to step 2;
    end if
  end if
end if
return Π

G. HEURISTIC

With the objective to mitigate the computational complexity of the above-mentioned optimal solution (ILP solution), we introduce an algorithm-based heuristic. The introduced algorithm considers user data rate, amount saving, battery charging level, extra power required, and vulnerability index. Accordingly, user utility function can be expressed as follows:

$$Z_{ij} = X_{ij} \cdot \varepsilon_{ij} \cdot \frac{S_{ij}}{P_{ij}^{cr}} \tag{25}$$

The algorithm aims to increase the benefits in terms of monetary saving over additional power consumption that would be required to use CR. As the algorithm's objective is to increase the benefit and decrease the cost, we named it "BC-algorithm". It should be noted that users here are originally connected to the MBS. However, the APs, which are covered by the MBS, have unutilized bands and are offering them, for a fee, to the users, named as CR-enabled users or secondary users (SUs). Using our proposed algorithm, the MBS will try to maximize the overall benefits for all users by short listing the users who benefit the most from their CR and allow them to access these APs via CR. In other words, the MBS has the upper hand in deciding who should participate and benefit from CR and who should refrain from participation.

In Algorithm , the MBS generates two lists. One list that contains the list of users who benefit the most Γ, and the other list, φ, contains users who should not be considered for the CR. Consequently, Algorithm is used to maximize the benefit of the total system.

As shown in Algorithm , Π represents the AP-SU assignment matrix, derived by the $(\hat{\Pi}, F) = new\_AP\_search$ (j^*, Π) algorithm. The flag F indicates whether $\hat{\Pi}$ is a more suitable AP-SUs assignment arrangement or not. In other words, if $F == 1$, $\hat{\Pi}$ is more suitable and vice verse. Algorithm begins with an initial assignment where each SU is assigned, allowed to access, a single AP. Then Algorithm adjusts the assignment of SUs to APs to maximize the value of the utility function during each iteration. To achieve this, during each iteration, Algorithm finds the SU with the lowest utility value and tries to locate another AP to increase the overall utility value of the network. If a new allocation is found, Algorithm begins a new iteration. However, if this is not achievable, Algorithm checks other SUs that are sharing the same AP with the SU one by one and finds an alternative better AP for them that can increase the overall utility value of the system. Upon finding this better AP, SU will be re-allocated to this AP. If the alternative AP is not found, Algorithm marks the SU and starts a new iteration until it finishes all users.

The recursive Algorithm is a crucial component for the BC-algorithm. Algorithm utilizes Algorithm to find a new AP for the chosen SU. In Algorithm , we presents $\bar{\Pi}$ as an intermediate AP-SUs assignment during a recursion. Algorithm checks the set of APs surrounding the chosen SU and the SU can access them. Subsequently, in each iteration Algorithm reallocates the chosen user to one of these APs and checks the overall utility function value. If it increases, it marks the AP and starts a new iteration until Algorithm marks all the AP for this SU and achieves the highest utility value. Then it returns the final assignment matrix to Algorithm . Consequently, Algorithm

Algorithm 3 $(\hat{\Pi}, F) = new\_AP\_search\ (j^*, \Pi)$

Set F=0, $\hat{\Pi} = \Pi$
Find $\bigcup_i = \{b|C_{i*,j} > min_{j\in Y_b} C_{ij}, b \in \bigcup\}$
if $\{C_{i*,j} > min_{j\in Y_b} C_{ij}, \exists b \in \bigcup\}$ **then**
  if $\{\Pi_{ij} = 1, \exists j \in \bigcup\}$ **then**
    Add AP-SU pair to jth pair and update Π;
  end if
  Mark the pair;
  for $b = 1 : |\bigcup_i|$ **do**
    if r_b not marked **then**
      Mark r_b
      if $\{j$ can access $r_b\}$ **then**
        update Π. set F==1
        Terminate
      else
        Find $Y_b = \{j|\Pi_{j,b} = 1, \Pi_{j,b} = 1, j \neq i, j \in \mathcal{J}\}$
        for $j = 1 : |Y_b|$ **do**
          $(\bar{\Pi}, F) = new\_AP\_search\ (j^*, \Pi)$;
          if F==1 **then**
            $\hat{\Pi} = \bar{\Pi}$;
            Terminate
          end if
        end for
      end if
    end if
    if F==1 **then**
      Add AP-SU pair to jth pair and update Π;
      Set $\hat{\Pi} = \Pi$
    end if
  end for
end if

chooses the next user and begins a new iteration and so on until it terminates.

The AP marking mechanism utilized in the above-mentioned algorithms reduces the computational-complexity while solving the AP-SUs allocation problem. Without using this marking mechanism, M^N iterations are required to locate the best AP-SUs bets allocation. However, in our case, the BC-algorithm requires M iterations maximum. Additionally, offloading unmarked SUs from marked AP to unmarked APs decreases the number of alternative APs for SUs and hence less computational processing power required. Hence, faster processing time.

H. COMPUTATIONAL COMPLEXITY ANALYSIS

In this section, we evaluate the computational complexity of our proposed Cognitive Radio heuristic. In Algorithm , we start with assuming that all N users require the CR access to the nearby APs. Hence, the algorithm sort the users according to their λ_{ij} and only users with λ_{ij} that is higher than a certain value A will be allowed to participate in the CR procedures. Thus, the computational complexity, up to this point, is $O(TNlogN)$.

Assuming that the number of the allowed users is N', each user from these N' users will be allowed to access the nearest BS. Subsequently, Algorithm starts with a flag F equals zero, and all the N' allowed users, which are grouped in Γ. Then, Algorithm finds the CR user with the minimum λ_{ij} and by using Algorithm , it tries to find another AP, from the available M APs, that can increase the user's λ_{ij} and yet increases the total benefit Z_{ij} at the same time to meet our objective function. Once AP is found the algorithm will mark the user, and go to the next user.

As mentioned before, Algorithm tends to determine the best AP to serve the selected user, and the algorithm has two Find-procedure, two For-loop procedure. However, Algorithm utilizes other procedures in Algorithm to validate if the new AP is suitable of not. Algorithm has two find-procedure, two For-loops. Accordingly, for Algorithm and Algorithm the computational complexity can be derived as $O(N'+M+M\cdot O(Algorithm\ ))$, and O($2M+M^2$), respectively.

Finally, presuming the worst case scenario where the heuristic searches all APs and users, the total heuristic complexity can be derived as $O(NlogN+N'+2M^2+M^3)$. where N represents the total number of users, N' number of users that were selected to participate in the CR procedures, and M is the number of available APs. Hence, the proposed heuristic algorithms are of the type pseudo polynomial time algorithm.

TABLE 2. Simulation parameters [13], [14], [54], [55].

Parameter	Value
PBSs number	1
SBSs number per PBS	4
SUs number per SBS	160
Power to transmit a bit	$1.75 \cdot 10^{-8}\ mW$
Power to switch channels	750 mW
Power to scan a channel	700 mW
Time to switch channels	0.06 ms
Time to scan a channel	500 ms
Packet mean rate	0.5 Packet/sec
Frequency of the Carrier	1900 MHz
Bandwidth of the Channel	10 MHz
Transmission Power of Macro BS	20 W
Transmission Power of APs	5 W
Battery power consumption co-efficient	1
Cost per bit for the MBS	$(1.20 : 1.86) \cdot 10^{-5}\$$
Cost per bit for APs	$(2.00 : 2.74) \cdot 10^{-5}\$$

IV. SIMULATION RESULTS AND DISCUSSION

To benchmark our approach, we implemented a hypothetical simulation scenario for the city of Perth as presented in Fig. 4. The simulation scenario was implemented in MATLAB R2019b using the simulation parameters in Table 2. In our simulation, users' packets generation followed a Poisson distribution with 0.5 as the mean rate [14]. The values of the "cost per bit" was obtained from one of

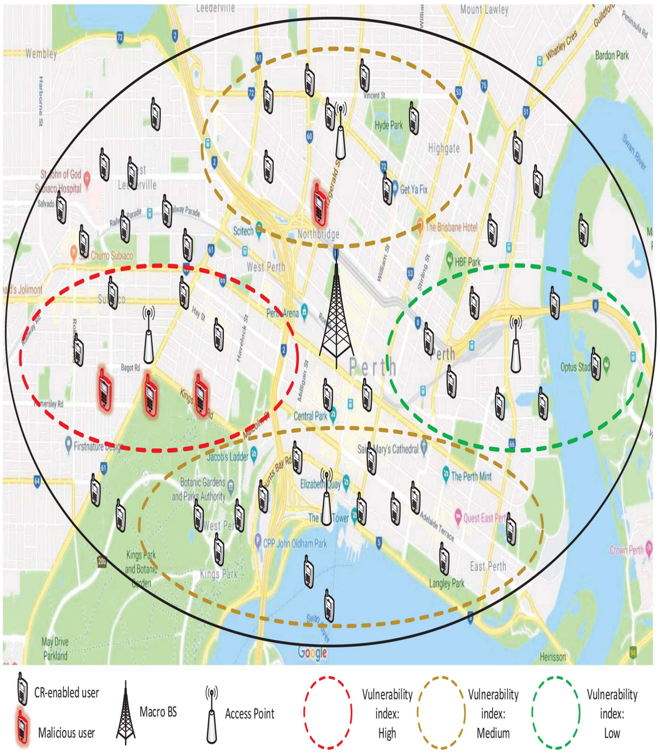

FIGURE 4. Hypothetical simulation scenario for the CR-based communication system - Perth, Western Australia.

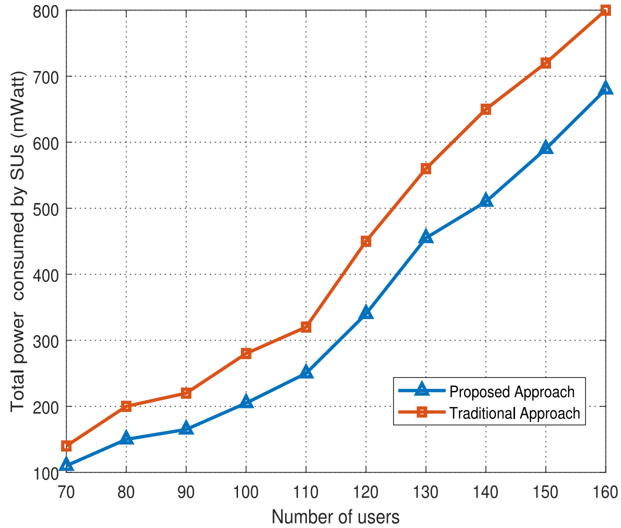

FIGURE 5. Total power consumed by SUs.

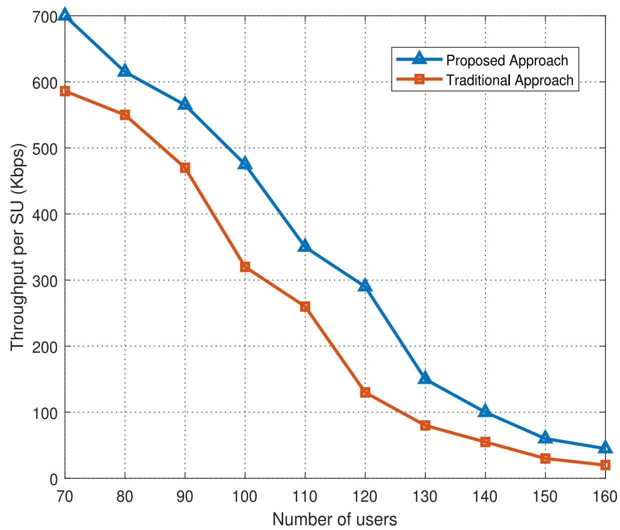

FIGURE 6. Secondary users' throughput.

the well-known operators in Australia [56]. In the simulated scenario, the radius of the macro base station was considered as 1000m and for the APs the radius was 200m [57]. Additionally, the number of users is set to range from 70 to 160. Such a range has been adopted in other research studies such as [58]–[60].

This section introduces the obtained simulation results and evaluates our proposed approach. Furthermore, it presents various comparisons between the proposed and the traditional CR approach [14], [54]. In the traditional approach, without any restrictions, all SUs are allowed to utilize their CR abilities to access any AP, irrespective of their battery level, traffic types, the AP's load, and AP's vulnerability level. However, unlike the traditional approach, our proposed approach shortlists SUs that benefit the most from the CR process and associates them to APs that increase the total benefit and yet meet the SUs requirements.

Fig. 5 presents a comparison between the traditional CR approach and our proposed approach in terms of total power consumed by SUs to send their data through the APs and the number of SUs influence on it. From Fig. 5, it is apparent that our proposed approach consumes less power in comparison to the traditional approach. This is because our proposed approach first shortlists SUs that benefit the most from the CR and then, in meeting its objective function (i.e., Eq. (17)), tends to associate the SUs with APs that require less CR power consumption to be accessed. Hence, the majority of SUs are served by the minimum possible CR power consumption. However, on the other hand, the traditional approach tends to allow all SUs, without restrictions, to access the APs and to associate SUs with the nearest AP, irrespective of the AP load or the CR power consumption to access it. This leads to more SUs competing on the available bands resulting in a higher CR power consumption.

Fig. 6 shows a comparison between the traditional approach and our CR proposed approach in terms of throughput per SU and the number of users' impact on this throughput. Based on the results displayed in Fig. 6, it is clear that our proposed approach provides higher throughput per SU than the traditional approach. This occurs because our proposed approach restricts the access to the APs, via CR, to the users who benefit the most from them leading to a fewer number of contending SUs which results in lower blocking probability and hence higher throughput. Additionally, in satisfying its objective function, our proposed approach

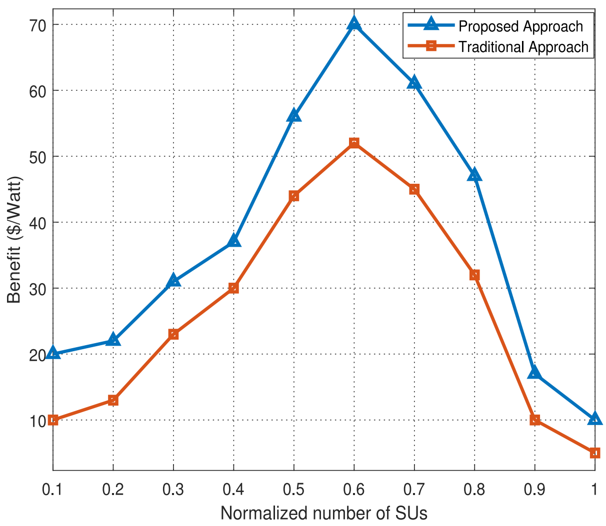

FIGURE 7. Secondary users' benefit.

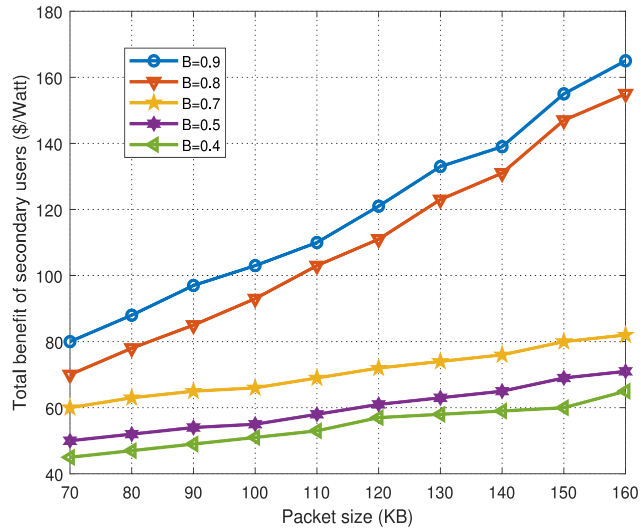

FIGURE 8. The impact on the benefit figure while changing the packet size.

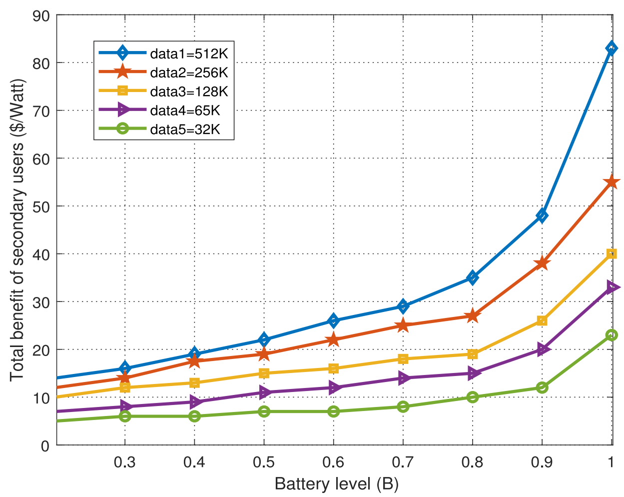

FIGURE 9. The influence on the benefit figure while changing the battery level.

shows a tendency to associate SUs to APs that have more free bands, which translates to higher data rates/throughput. However, in the traditional approach, all SUs are allowed to access their nearest APs, irrespective of the number of available free bands at these APs and the APs' load. This leads to a high level of contention between the SUs on the free bands and results in high blocking probability, which translates to lower throughput.

Fig. 7 displays the impact of the normalized number of users on the total benefit figure of the system, where the normalized number of users represents the ratio between the number of actual participating SUs to the total number of SUs who can access APs, using their CR abilities. For instance, a normalized value of 0.1 means allowing only 10% of total SUs to access APs by using their CR abilities. Additionally, in this context, Fig. 7 compares the traditional approach with our approach. Based on the results in Fig. 7, it salient that our proposed approach achieves higher benefit figures than the traditional approach. This is because our proposed approach, in meeting its objective function (i.e., Eq. (17)), associates SUs to APs that maximize the overall benefit and yet meet SUs requirements. Such an approach balances the load between APs and alleviates the contention level at each AP which means less CR power consumption and higher throughput. This results in high overall benefit for our proposed approach. However, unlike our proposed approach, the traditional approach tends to associate SUs to their nearest APs, irrespective of the APs' load and the CR power consumption to access them. This results in some APs become overloaded and increases the level of contention among SUs on the available bands at these APs. Consequently, this leads to a higher CR power consumption and less throughput, hence less overall benefit. Fig. 7 shows also that increasing the number of SUs accessing the APs will increase benefit until some point where the level of contention between SUs becomes very high and overwhelms the benefit. At this point, the benefit figure starts to decline.

Additionally, in this paper, we examined the influence of the size of the data, battery level, and users' confidentiality index on the total benefit of the SUs. Fig. 8 shows the influence of increasing the size of the data packet, that SUs send through the APs via CR, on the total benefit figure. Additionally, Fig. 8 presents that influence under different battery levels. The figure manifests that for small packet sizes and low battery levels, SUs' benefits are lower compared to the situation where SUs' battery levels are high and sending relatively large packets. This occurs because the extra power required for the CR technique is more precious for low battery users and, hence, the power cost is too high for them, resulting in less net-benefit for them.

Fig. 9 illustrates the impact of increasing the battery level of the SUs on the total benefit figure. Furthermore, it shows that impact while using different sizes of data. Based on the obtained results in Fig. 9, it is evident that increasing the battery level of the SUs improves the SUs benefits figure.

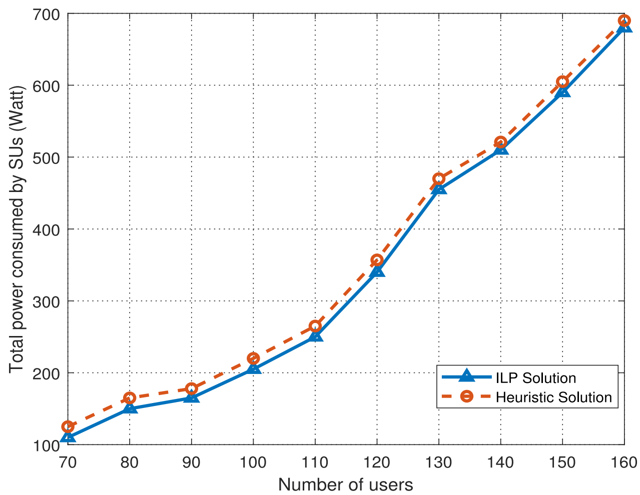

FIGURE 10. Heuristic simulation results: power consumption.

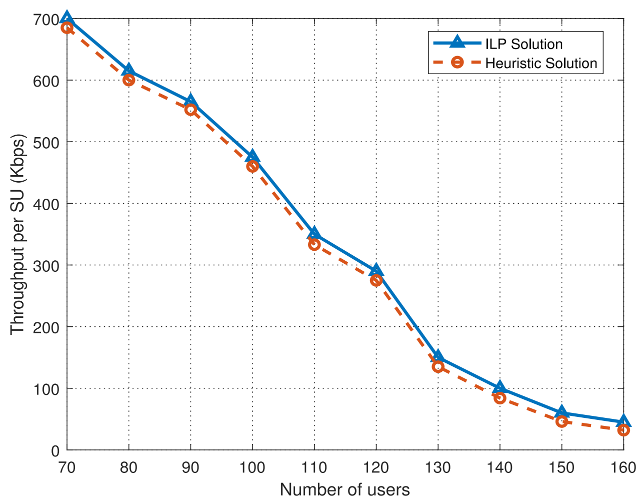

FIGURE 11. Heuristic simulation results: throughput.

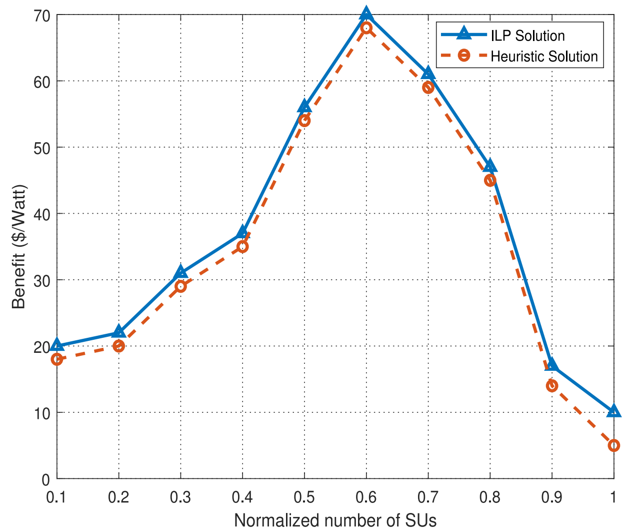

FIGURE 12. Heuristic simulation results: total benefit.

TABLE 3. Summary of the findings.

Cognitive radio Technique	Total Power Consumed By SUs (Watt)	Throughput/SU (Kbps)	APs Spectrum Utilization (%)
Traditional approach [14], [54]	808	586	88
Proposed approach	680	703	98

However, using larger data sizes boosts the benefit figure even more. This occurs because, for SUs with abundant power resource, the CR power cost is easily affordable and larger data size means larger savings, thus the benefit figure is high.

Fig. 10 shows a comparison between the integer linear programming (ILP) solution obtained via CPLEX, and our proposed heuristic solution in terms of total power consumed by SUs. From Fig. 10, it is evident that our proposed heuristic consumes marginally higher power than the ILP solution. On the other hand, Fig. 11 presents a comparison between the ILP solution and our proposed heuristic in terms of throughput per SU. From Fig. 11, it is notable that the proposed heuristic offers slightly less throughput than the ILP solution. Furthermore, Fig. 12 illustrates a comparison between our proposed heuristic and the ILP solution in terms of total benefit figure. From Fig. 12, it is evident that our proposed heuristic offers almost identical benefit to the ILP solution. From Fig. 10, 11, and 12 it is notable that our heuristic can used to attain near-optimal results for the above-mentioned research problem.

Table 3 summarizes our findings in this work. The table introduces a comparison between the traditional CR approach and our proposed approach. As demonstrated in Table 3 the proposed approach consumes less power compared to the traditional approach. Additionally, our proposed approach offers higher throughput. It also achieves better utilization for the APs unutilized spectrum.

V. CONCLUSION

Owing to its multi-dimensional awareness and ability to sense, learn and decide subsequent actions, the cognitive radio technique, supported by the software defined radio technology, offers great potential to fulfill users' ever-increasing demands and mitigate the looming problem of spectrum scarcity. However, due to its power-hungry procedures and security risks, these offered benefits can be overwhelmed by the costs associated with extra power requirements and/or security breaches. In this paper, we introduced a new cognitive radio communication approach that maximizes the users' benefits while taking the power consumption and security risk into consideration. Furthermore, while quantifying the benefit figures, our proposed approach considered the device's battery level, type of traffic, vulnerability level of the accessed network, and the number of free bands in the accessed spectrum. The obtained results showed that the proposed approach saved up to 18% of the power consumption, increased the total throughput per user by 20%, and provided better spectrum utilization reaching up to 98%. This research study opens a new research area towards safer and greener cognitive radio solutions. For instance, our future work will investigate how to extend this paper to utilize the powerful computation capabilities of cloud computing to rapidly predict and detect available bands and its suitability in terms of SUs' security and quality requirements. Such an approach will offload the computational complexity, and its corresponding power consumption, from the BSs to the cloud resulting in less power reduction. Additionally, the decisions on which SUs access which bands and for how long will be processed faster, more efficient, and securely leading to less power to be consumed and more efficient and secure way of handling the radio spectrum.

REFERENCES

[1] "Cisco visual networking index: Global mobile data traffic forecast update, 2017–2022," Cisco, San Jose, CA, USA, Rep., 2019. [Online]. Available: https://www.cisco.com/c/dam/m/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf

[2] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[3] X. Hong, J. Wang, C.-X. Wang, and J. Shi, "Cognitive radio in 5G: A perspective on energy-spectral efficiency trade-off," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 46–53, Jul. 2014.

[4] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 5–23, Feb. 2011.

[5] C. Jiang, H. Zhang, Y. Ren, and H.-H. Chen, "Energy-efficient noncooperative cognitive radio networks: micro, meso, and macro views," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 14–20, Jul. 2014.

[6] M. R. Hassan, G. C. Karmakar, J. Kamruzzaman, and B. Srinivasan, "Exclusive use spectrum access trading models in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2192–2231, 4th Quart., 2017.

[7] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, and B. Ottersten, "Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 674–707, 1st Quart., 2017.

[8] H. Cui, V. C. M. Leung, S. Li, and X. Wang, "LTE in the unlicensed band: Overview, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 99–105, Aug. 2017.

[9] B. Chen, J. Chen, Y. Gao, and J. Zhang, "Coexistence of LTE and Wi-Fi on 5 GHz with corresponding deployment scenarios: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 7–32, 1st Quart., 2017.

[10] G. Naik, J. Liu, and J.-M. J. Park, "Coexistence of wireless technologies in the 5 GHz bands: A survey of existing solutions and a roadmap for future research," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1777–1798, 3rd Quart., 2018.

[11] D. Zhang *et al.*, "Energy-harvesting-aided spectrum sensing and data transmission in heterogeneous cognitive radio sensor network," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 831–843, Jan. 2017.

[12] M. R. Mili, L. Musavian, K. A. Hamdi, and F. Marvasti, "How to increase energy efficiency in cognitive radio networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1829–1843, May 2016.

[13] H. Khaled, I. Ahmad, D. Habibi, and Q. V. Phung, "An energy-aware cognitive radio-based communication approach for next generation wireless networks," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun. IEEE 17th Int. Conf. Smart City IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, 2019, pp. 1817–1824.

[14] E. F. Orumwense, T. J. Afullo, and V. M. Srivastava, "Secondary user energy consumption in cognitive radio networks," in *Proc. IEEE AFRICON*, 2015, pp. 1–5.

[15] *IEEE Standard for Safety Levels With Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 KHz to 300 GHz.* [Online]. Available: http://emfguide.itu.int/pdfs/C95.1-2005.pdf

[16] M. R. Amini, M. Mahdavi, and M. J. Omidi, "Discrete-time Markov chain analysis of energy efficiency in a CR network regarding primary and secondary traffic with primary user returns," *IEEE Access*, vol. 6, pp. 22305–22323, 2018.

[17] X. Tang, P.-E. Gaillardon, and G. De Micheli, "A high-performance low-power near-VT RRAM-based FPGA," in *Proc. IEEE Int. Conf. Field Program. Technol. (FPT)*, 2014, pp. 207–214.

[18] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Commun.*, vol. 12, no. 3, pp. 132–150, 2015.

[19] 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, 2nd Quart., 2014.

[20] J. Zhang, G. Pan, and H.-M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, 2016.

[21] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2016.

[22] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013.

[23] A. Roy, S. Midya, K. Majumder, S. Phadikar, and A. Dasgupta, "Optimized secondary user selection for quality of service enhancement of two-tier multi-user cognitive radio network: A game theoretic approach," *Comput. Netw.*, vol. 123, pp. 1–18, Aug. 2017.

[24] N. D. Chatzidiamantis, E. Matskani, L. Georgiadis, I. Koutsopoulos, and L. Tassiulas, "Optimal primary-secondary user cooperation policies in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3443–3455, Jun. 2015.

[25] A. Gouissem, R. Hamila, N. Aldhahir, and S. Foufou, "Secondary users selection and sparse narrow-band interference mitigation in cognitive radio networks," *Comput. Commun.*, vol. 123, pp. 97–115, Jun. 2018.

[26] G. Ding *et al.*, "Spectrum inference in cognitive radio networks: Algorithms and applications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 150–182, 1st Quart., 2017.

[27] Z. Khan, J. J. Lehtomäki, L. A. DaSilva, E. Hossain, and M. Latva-Aho, "Opportunistic channel selection by cognitive wireless nodes under imperfect observations and limited memory: A repeated game model," *IEEE Trans. Mobile Comput.*, vol. 15, no. 1, pp. 173–187, Jan. 2016.

[28] G. Yang *et al.*, "Cooperative spectrum sensing in heterogeneous cognitive radio networks based on normalized energy detection," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1452–1463, Mar. 2016.

[29] A. Ali and W. Hamouda, "Advances on spectrum sensing for cognitive radio networks: Theory and applications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1277–1304, 2nd Quart., 2017.

[30] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

[31] M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," *J. Inf. Security Appl.*, vol. 38, pp. 40–49, Feb. 2019.

[32] K. An, M. Lin, J. Ouyang, and W.-P. Zhu, "Secure transmission in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 3025–3037, Nov. 2016.

[33] M. Jo, L. Han, D. Kim, and H. P. In, "Selfish attacks and detection in cognitive radio ad-hoc networks," *IEEE Netw.*, vol. 27, no. 3, pp. 46–50, May/Jun. 2013.

[34] S. Chatterjee, S. P. Maity, and T. Acharya, "Energy-spectrum efficiency trade-off in energy harvesting cooperative cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 295–303, Jun. 2019.

[35] M. Yousefvand, T. Han, N. Ansari, and A. Khreishah, "Distributed energy-spectrum trading in green cognitive radio cellular networks," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 3, pp. 253–263, Sep. 2017.

[36] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Trans. Cogn. Commun. Netw.*, vol. 2, no. 2, pp. 110–128, Jun. 2016.

[37] X. Huang, T. Han, and N. Ansari, "On green-energy-powered cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 827–842, 2nd Quart., 2015.

[38] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.2793, 2012.

[39] S. Xu, Y. Li, Y. Gao, Y. Liu, and H. Gačanin, "Opportunistic coexistence of LTE and WiFi for future 5G system: Experimental performance evaluation and analysis," *IEEE Access*, vol. 6, pp. 8725–8741, 2018.

[40] R. Zhang, M. Wang, L. X. Cai, Z. Zheng, X. Shen, and L.-L. Xie, "LTE-unlicensed: The future of spectrum aggregation for cellular networks," *IEEE Wireless Commun.*, vol. 22, no. 3, pp. 150–159, Jun. 2015.

[41] *Multefire Release 1.0 Technical Paper: A New Way to Wireless*. Accessed: Oct. 1, 2019. [Online]. Available: https://www.multefire.org/wp-content/uploads/MulteFire-Release-1.0-whitepaper_FINAL.pdf

[42] C. Rosa, M. Kuusela, F. Frederiksen, and K. I. Pedersen, "Standalone LTE in unlicensed spectrum: Radio challenges, solutions, and performance of multefire," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 170–177, Oct. 2018.

[43] Y. Gu, H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Minimizing age of information in cognitive radio-based IoT systems: Underlay or overlay?" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10273–10288, Dec. 2019.

[44] S. Sun, Y. Ju, and Y. Yamao, "Overlay cognitive radio OFDM system for 4G cellular networks," *IEEE Wireless Commun.*, vol. 20, no. 2, pp. 68–73, Apr. 2013.

[45] W. Liang, K. Di Wang, J. Shi, L. Li, and G. K. Karagiannidis, "Distributed sequential coalition formation algorithm for spectrum allocation in underlay cognitive radio networks," *IEEE Access*, vol. 7, pp. 56803–56816, 2019.

[46] L. Xiang, D. W. K. Ng, R. Schober, and V. W. Wong, "Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 736–751, Feb. 2018.

[47] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 4th Quart., 2020.

[48] T. Han and N. Ansari, "A traffic load balancing framework for software-defined radio access networks powered by hybrid energy sources," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 1038–1051, Apr. 2016.

[49] Q. Ye, B. Rong, Y. Chen, M. Al-Shalash, C. Caramanis, and J. G. Andrews, "User association for load balancing in heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2706–2716, Jun. 2014.

[50] H. Kim, G. De Veciana, X. Yang, and M. Venkatachalam, "Distributed *alpha*-optimal user association and cell load balancing in wireless networks," *IEEE/ACM Trans. Netw.*, vol. 20, no. 1, pp. 177–190, Feb. 2012.

[51] Y. Wu, Y. He, L. P. Qian, J. Huang, and X. Shen, "Optimal resource allocations for mobile data offloading via dual-connectivity," *IEEE Trans. Mobile Comput.*, vol. 17, no. 10, pp. 2349–2365, Oct. 2018.

[52] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model," *IEEE Trans. Ind. Informat.*, vol. 14, no. 3, pp. 1220–1231, Mar. 2018.

[53] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[54] V. Namboodiri, "Are cognitive radios energy efficient? A study of the wireless LAN scenario," in *Proc. IEEE 28th Int. Perform. Comput. Commun. Conf. (IPCCC)*, 2012, pp. 437–442.

[55] M. Ismail, W. Zhuang, E. Serpedin, and K. Qaraqe, "A survey on green mobile networking: From the perspectives of network operators and mobile users," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1535–1556, 3rd Quart., 2016.

[56] *Optus Australia*. Accessed: Oct. 3, 2019. [Online]. Available: https://www.optus.com.au

[57] Q. Fan and N. Ansari, "Towards throughput aware and energy aware traffic load balancing in heterogeneous networks with hybrid power supplies," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 4, pp. 890–898, Dec. 2018.

[58] A. Mesodiakaki, F. Adelantado, L. Alonso, and C. Verikoukis, "Energy-efficient user association in cognitive heterogeneous networks," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 22–29, Jul. 2014.

[59] X. Liu and N. Ansari, "Profit-driven user association and smart grid energy transfer in green cellular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10111–10120, Oct. 2019.

[60] J. Opadere, Q. Liu, T. Han, and N. Ansari, "Energy-efficient virtual radio access networks for multi-operators cooperative cellular networks," *IEEE Trans. Green Commun. Netw.*, vol. 3, no. 3, pp. 603–614, Sep. 2019.

HAITHAM KHALED (Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering in 2006, and the M.Eng. degree in 2016. He is currently pursuing the Ph.D. degree with Edith Cowan University, Australia. His research interests include green communications, wireless networks, and 5G technologies.

IFTEKHAR AHMAD (Member, IEEE) received the Ph.D. degree in communication networks from Monash University, Australia, in 2007. He is currently an Associate Professor with the School of Engineering, Edith Cowan University, Australia. His research interests include, machine learning, localisation, sensor fusion, sports science, QoS in communication networks, software-defined radio, wireless sensor networks, and computational intelligence.

DARYOUSH HABIBI (Senior Member, IEEE) received the Bachelor of Engineering (electrical) degree (First Class Hons.) and the Ph.D. degree from the University of Tasmania in 1989 and 1994, respectively. His employment history includes Telstra Research Laboratories, Flinders University, Intelligent Pixels, Inc., and Edith Cowan University, where he is currently a Professor and the Executive Dean of engineering. His research interests include engineering design for sustainable development, reliability and quality of service in communication systems and networks, smart energy systems, and environmental monitoring technologies. He is a Fellow of Engineers Australia and the Institution for Marine Engineering, Science and Technology.

QUOC VIET PHUNG (Member, IEEE) is a Research Fellow with the School of Engineering, Edith Cowan University. His research background is in electronics and communications. He has been leading and conducting a number of research and development projects on automotive, agricultural and renewable industries. These have involved both hardware and software development, which mainly involves ground-based remote sensing, data acquisition, optimization using pattern recognition and machine learning, and IoT platform. His research is shipping to tackle new challenges in next generation of communication technologies. The research theme is the merging of wireless communication, security and artificial intelligent solutions.