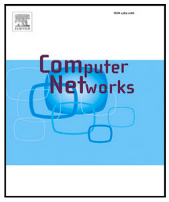
Computer Networks 254 (2024) 110818

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Cognisseum: Cognitive radios on Colosseum facing adversaries☆

Sayanta Seth [a,1,*], Debashri Roy [b], Murat Yuksel [c]

[a] Department of Electrical and Computer Engineering, North Carolina State University, NC, USA
[b] Department of Computer Science and Engineering, The University of Texas Arlington, TX, USA
[c] Department of Electrical and Computer Engineering, University of Central Florida, FL, USA

ARTICLE INFO

Keywords:
Cognitive radio
Spectrum access
Coalition formation
Colosseum

ABSTRACT

Cognitive radio technology brings a lot of interesting features which affect the transmission and reception properties of modern communication devices. Dynamic spectrum sensing, channel hopping and allocation, and software-based control are among the many. The new features allow strategic defense mechanisms while also enabling more capable adversarial attacks. In this work, we study coalitions of secondary users (SUs) against adversaries. In the presence of primary users (PUs), we inspect the behavior of SU pairs in cognitive radio networks, before and after adversarial attacks. We propose algorithms for forming coalitions among SU pairs. We consider two attack strategies for the adversaries: smart or naïve. We study how the channels are allocated if there is an attack and how the payoffs of those SU pairs vary with varying number of channels. We also show the effects of attack from the attackers' point-of-view and how the attack strategy changes if the adversaries act smart vs. naïve. Using Colosseum, a large-scale wireless channel emulator, we construct a functional cognitive radio network and use its software-defined radio (SDR) hardware as SU and adversarial nodes. Using this setup, we run experiments and record data by running network performance measurement tool `iPerf3` for various coalitional setups.

1. Introduction

A network of unlicensed users that dynamically detect unused licensed spectrum for their own use without interfering licensed users is called a cognitive radio network (CRN). CRNs promise to deliver an intelligent solution to the issues in conventional wireless technology related to their limited and under-utilized spectrum [2]. Despite these promises that CRNs bring on paper, there is a need to conduct extensive studies, simulation and real-world experiments to validate their effectiveness in solving the spectrum under-utilization challenge. There exists two types of users [3] in a CRN: Primary Users (PUs), who are licensed owners of the specific frequency spectrum in question, and Secondary users (SUs), who opportunistically exploit the unoccupied licensed spectrum. In the United States, according to Federal Communications Commission (FCC) [4,5], most of the radio spectrum is used inefficiently, which results in over-utilization of many of its bands [6]. For example, in most places around the globe, cellular bands have become very congested due to high demand from civilian applications. Whereas, other bands exclusively utilized by military equipment and paging devices are under-utilized most of the time in most places. CRNs attempt to alleviate the problem of spectrum under-utilization by letting the SUs utilize the bands allocated to PUs in a way such that the PU communications are not compromised. The SUs temporarily using the PU channels must immediately vacate the channel whenever required by the legal channel owner [6].

Impact of adversaries in CRN: Consideration of adversaries on CRNs changes the dynamics significantly. An attacker trying to degrade the performance of a CRN can block the channels being used by SUs. Recent work [7] studied the performance of CRNs when there is a single attacker eavesdropping the transmission among SUs. However, to our knowledge, the case of multiple SUs being attacked by multiple adversaries has not been considered.

Our Focus: In this paper, we follow the general concept of CRN by allowing SUs to opportunistically use the shared spectrum with the PUs. However, there is a plethora of researches on such opportunistic channel allocation between the primary and secondary users, e.g., [8,9]. Different from those studies, our paper is focused on maximizing the channel utilization for the channels allocated to the SUs in the presence

☆ A preliminary version of this work was published in Seth et al. (2021) [1]. This manuscript significantly extends the preliminary version by adding experiments on the Colosseum testbed.

* Corresponding author.
E-mail addresses: sseth2@ncsu.edu (S. Seth), debashri.roy@uta.edu (D. Roy), murat.yuksel@ucf.edu (M. Yuksel).

[1] Dr. Seth was with the University of Central Florida during most of this work.

https://doi.org/10.1016/j.comnet.2024.110818
Received 23 October 2023; Received in revised form 2 July 2024; Accepted 17 September 2024
Available online 23 September 2024

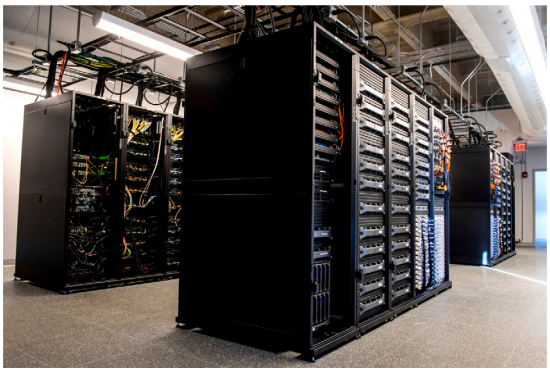


Fig. 1. Colosseum [11]: High-performance USRP devices arranged in stacks known as 'quads'.

of multiple adversaries trying to block the SUs. We focus on a CRN design where each SU transmits based on its power budget. We consider an SU transmitter and SU receiver to be a single entity, henceforth referred to as an 'SU pair'. For simplicity, we assume that there is a fixed number of PUs which are always present and are constantly accessing their own channels. We further assume that the channels being used by the PUs are known. The remaining channels get allocated to the *SU coalitions*.

Benefit of a Coalition: By design, when the SU pairs work together to maximize their overall payoff, we determine that they have formed a coalition. Our proposed coalition modeling methodology increases channel availability to the SU pairs when they are part of a coalition rather than staying as a single SU pair. This increases the likelihood of non-starvation of SU pairs (in terms of channels) in case of adversarial attack. The adversaries considered in the system, are capable of only attacking the SU pairs, and not the PUs, following the FCC mandated rules [10]. We consider the problem of tuning transmission power of such SU pairs under the presence of multiple adversaries. We use this transmission power criterion to decide the coalition formation of the SU pairs. *Overall, we consider a game-theoretic framework to study the multi-SU-pair multi-adversary scenario in CRNs. We design an algorithm for SU pairs to form coalitions to maximize their payoffs/utilities, i.e., throughput among them. Further, we study, using simulations, the stability of the coalitions formed and record the total value of all coalitions in terms of the total throughput (i.e., sum rate) in the presence of adversarial attack.*

Cognisseum Framework: Beyond the simulation-based study of the concept [1], we focus on developing a CRN framework in the presence of adversaries on Colosseum (refer to Fig. 1), which is the world's largest wireless emulator with 256 software-defined radios (SDRs) to emulate up to 65,536 100 MHz-RF channels [11]. The SUs are implemented on real USRP devices that can be accessed via Colosseum. To the best of our knowledge, this is the first study to present coalitional cognitive radios on Colosseum, which we name *Cognisseum*. In Cognisseum, we focus on already-formed coalitions consisting of SU pairs, each being initialized with a number of non-overlapping channels. After running emulation for some time, we introduce adversarial presence and record the before and after attack throughputs. This hardware-based emulation will serve as a benchmark in the field of dynamic spectrum access (DSA) by cognitive radios facing adversaries.

The main contributions of our work are as follows:

(1) We propose an intelligent coalition formation algorithm without overlapping transmission power radii, ensuring communication interference is avoided.
(2) We devise an adversarial coalition formation algorithm, keeping in mind the smart and naïve attack strategies of the proposed framework.
(3) We present a stability criterion for the convergence of the coalition formation algorithm, so that the SUs maintain coalitions according to their payoffs.
(4) We perform hardware emulation on Colosseum, a large-scale wireless emulator. Using real USRP devices, we show how wireless channels of various pathloss values affect the sum rate of the coalition sets.
(5) On Colosseum, we emulate an adversarial network and show how legitimate radios can improve their payoff by switching coalitions after being attacked by an adversary.

Key insights from our study include:

(1) In simulation, we show how the average utilities of the SU pairs vary: After attack, the average coalitional utility suffers by about 200% with adversary count increasing by 120%. We also demonstrate that coalition utility increases by about 176% while increasing channel count by about 192%, for constant number of adversaries.
(2) We observe, for the same number of SU pairs and channels, the average coalitional utilities decrease with increasing adversary count.
(3) We observe that smart attack strategy unleashes more damage on the proposed framework when compared to the naïve one.
(4) We observe the marginal benefits of increasing channel count versus increasing the SU pair knowledge about PU activity in the CRN.
(5) In emulation, we show how we can utilize Colosseum as a wireless test-bed for our setup.
(6) We observe significant improvement in overall coalition throughput (sum rate) after the affected pair switches coalition.

Organization of the Paper: The rest of the paper is arranged as follows: In Section 2, we discuss the recent findings in CRN in general including power and sub-channel allocation techniques, Nash-bargaining games and mechanisms of spectrum sensing. In Section 3, we describe the Cognisseum system model and necessary assumptions for simulation and emulation, along with the need for coalition formation among SU pairs. In Section 4, we talk about the Cognisseum game theoretic framework, and discuss about the payoff function calculation and our novel coalition formation algorithms. In this section, we also introduce the concept of the adversaries in the system. In Section 5, we chalk out the details about our two-fold approach of software-based simulation and Colosseum-based emulations. Here, we go in detail about the Colosseum framework and how it functions. We also show the Colosseum parameters and channel conditions that we have used in our experiments. Detailed experimental results are presented in Sections 4.4.2 and 5.4, where we categorically discuss each of the plots pertaining to the simulation and emulation parts of the experiments respectively. Finally, our findings are summarized in Section 6.

2. Related work

DSA and CRNs have been a hot topic in wireless communications and information theory over the last two decades and the availability of software-defined radios has enabled significant leaps in research and development in this area. DSA in millimeter wave (mmWave) bands has been extensively studied in the literature [12–17]. In CRNs, it is crucial for an SU to predict with high accuracy when the PU arrives so that it can vacate its band without much impact on the PU. Hence, most of the literature focused on improving this prediction and reducing the interference on the PUs. Since SUs are competing for the unused spectral resources, the contention among them attracted significant attention from researchers. Centralized and distributed spectrum sensing models were proposed [18–21]. These techniques employed a novel power allocation scheme that uses dynamic sub-channel method based on a Nash Bargaining game among SUs. In a similar vein, Saad et al. [22,23]

introduced the idea of cooperative spectrum sensing among SUs for single-PU scenario, where the SUs increase their sensing accuracy by participating in a coalitional game. The authors explored the trade-off between the probability of detecting the PU and the probability of false alarm on the SU network topology and dynamics. These efforts focused on reducing the interference on PUs via various mechanisms of spectrum sensing and SU coordination. Different strategies of PU–SU interaction are well investigated. Many studies considered game-theoretic approaches to capture the strategies of the SUs in presence of the PUs. The studies outlined application of game theory to the SU strategy design and showed how non-cooperative [24–26] and cooperative [27,28] games can be used as tools to model the PU–SU interaction of cognitive radios. In a cognitive radio environment, it is crucial for an SU to anticipate with a high probability when the PU arrives so that it can vacate its band without much impact on the PU. Hence, effective sensing of the spectrum and learning and predicting the spectrum usage patterns of the PUs attracted a lot of attention.

Spectrum (usage) prediction is another area where a lot of research has been conducted. The two widely used spectrum prediction techniques are local and cooperative spectrum prediction. In the local spectrum prediction, the SU uses a Hidden Markov model to predict the status of the current channel in which it functions. Based on its prediction, it may switch to another channel when needed. The cooperative technique is where the selfish SUs might have to form a coalition to increase their individual payoffs. Cooperative spectrum sensing in CRNs with single PU has been studied in [22]. Further, significant work have been conducted on centralized collaborative sensing, where, given the mobile ad hoc nature of the cognitive radio users, a distributed game-theoretic framework has been proposed which reduces the average probability of the false detection of the PU significantly compared to the non-cooperative sensing.

Novelty of Cognisseum: Large literature can be found focusing on game-theoretic modeling of the PU–SU interaction, in both centralized and distributed manners. Our work takes these approaches and formulates the activities of SUs in the presence of multiple adversaries. We propose a novel framework where SUs cooperatively form coalitions in a dynamic manner to increase the payoffs of the coalition as a whole. Initial experimentation using the Colosseum platform have been covered extensively in [29,30]. These papers show us how to utilize the wireless channel emulator for a variety of scenarios. In other words, they are more of tutorial in nature. To the authors' best of knowledge, proper utilization and experimentation using this platform on a CRN has not yet been performed. In this paper, we aim to show how real-world version of cognitive radios can be implemented on Colosseum and perform extensive experiments on this Cognisseum system.

3. Cognisseum: System model and assumptions

We consider a 2-dimensional geographical plane for CRN nodes. The system is pre-occupied by $\mathcal{T}$ PUs and multiple SUs.

PU Modeling: We model the $\mathcal{T}$ PUs to frequently access some specific sub-channels, while leaving the remaining sub-channels empty during a particular time period in the day. The authors in [31] have given an example of the Disney TV channel as a PU that is active for 75% of the time during the day, which shows frequent and almost continuous PU activity on its own licensed spectrum. In this research, we assume that the frequent on-off activity and the channel utilization of the PUs is known by the SU pairs with a probability Q. Since each SU pair is made up of a single transceiver, devoid of interference, we simply multiply Q with the link rate R for each practicable link. For example, if $Q = 0.5$, then the SU pairs can successfully predict PU activity in the system 50% of the time. During that time of the day, the SUs can use those remaining sub-channels for their communication, which enables us to run our SU-based experiments during that time.

SU Modeling: The CRN system also consists of multiple legitimate SU radios are then categorized into equal number of transmitters and receivers and formed into pairs, each called an 'SU pair'. Each of the transmitter and the receiver of the SU pairs is assumed to have a *virtual proximity area* directly proportional to their power radii. The transmit power of each node is provided as an input and it is initialized as a random positive value uniformly distributed between 0 and 1 Watt. In proportion to the randomly chosen power value, the power radius is drawn. Referring to Fig. 2(a), we can see that the overall power radii of a transmitter SU and a receiver SU, comprising of the pair. Here, it is important to clarify that we assume short time intervals when these transceiver pairs are scheduled to transmit and receive respectively. From this, we build up the notion of an SU pair, which has a single transceiver, imposing the requirement of having pairs of individual SUs when forming a coalition. When two SUs are exchanging data they have to dedicate their transceivers to only one wireless link, at any point in time. Overall, this requires the number of SUs that are actively transmitting/receiving data to be in multiples of 2. We represent such legitimate SU pairs as $\mathcal{N} = \{N_1, N_2, \ldots, N_\eta\}$ which are initialized with varying power budget, denoted by the set $\mathcal{P} = \{P_{N_1}, P_{N_2} \ldots P_{N_\eta}\}$ respectively.

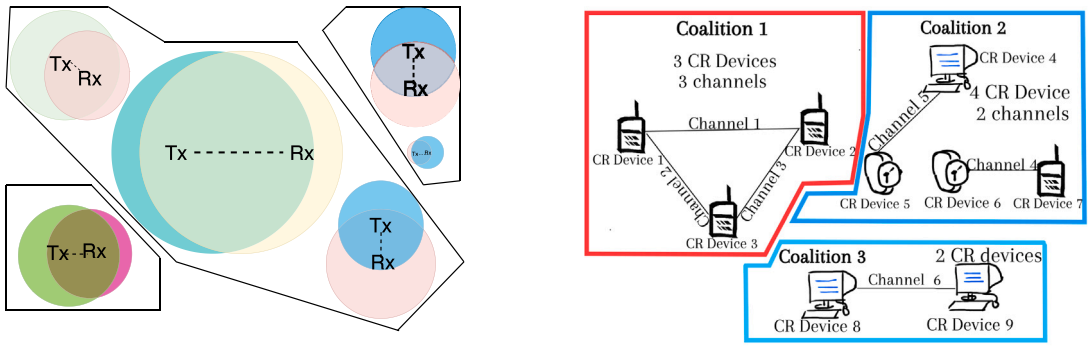
3.1. SU coalition modeling

Coalition Formation: We assume that SUs form coalitions to better utilize the available bandwidth in the presence of attackers trying to bring down their effective bandwidth. In Fig. 2(a), we show how SU pairs form coalitions. Fig. 2(b) shows a typical scenario of such cooperative behavior, where SUs (devices) are shown to form three different coalitions. The red coalition has three CRN devices in it. As per the system model, this is not possible because even in a singleton, there must be at least two SUs, as we have considered an SU pair to be a single entity. Within a SU pair, the SU transmitter and receiver communicate on the same sub-channel and this sub-channel is treated as a shared communication medium internally. However, within a coalition, our model assumes no communication among SU pairs whatsoever. The SU pairs simply communicate internally using their subchannels (they may choose to time share their subchannels if need arises, e.g., under adversarial attack scenario). The rest of the coalitions in blue are feasible because both of them have SUs in multiples of two.

Inter-Coalition Communication: Following the standard, we use the Common Control Channel (CCC) [32] for inter-coalition communication. When the SU pairs associate themselves to a coalitions, all of them can maintain communication among themselves via CCC. The coalitions use the CCC to decide whether to join or leave a coalition in the event of an attack. For example, SU pairs of a coalition might want to be part of a bigger coalition when they feel vulnerability to adversarial attacks. An adversarial attack could signify that the attacked coalition might be left without any channel to communicate. If the attacked coalition joins another coalition, then it is likely that its SU pairs can transmit using the existing channel(s), which becomes an incentive to join a bigger coalition. We design Cognisseum to be adaptive to the existing CRN deployment, hence we use the pre-existing spectrum sensing database [33] or methodologies determining the PU presence [32]. Hence, we do not consider spectrum sensing information exchange through the CCC in our framework.

3.2. Channel allocation schemes

We assume that a total of W Hz is the available bandwidth to the coalitions of SU pairs. This does not include the bandwidth the PUs are frequently using as we assume that the channels PUs are using are known with a probability P. The total bandwidth W is further divided into $C = |\mathcal{N}|/2$ non-overlapping sub-channels, where $|\mathcal{N}|/2$ refers to the total number of SU pairs formed. Hence, each SU pair gets one sub-channel initially.



(a) SU pair coalition formation based on power radii

(b) Coalition formation among SU pairs

Fig. 2. Coalition formation concepts in Cognisseum. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Now, we test our coalition formation model under two different channel allocation strategies: smart and naive. In the smart scheme, the number of channels allocated to coalitions is directly proportional to the number of SU pairs present in a particular coalition. For example, if there are 10 SU pairs formed into 5 coalitions with each coalition consisting of 2 SU pairs. Since there will be 10 sub-channels, then each coalition will get 2 sub-channels. But under real-world circumstances, the channel allocation might not be as expected, and in some cases, coalitions can end up receiving a very small number of channels compared to the number of SU pairs present in them. However, if the number of channels is greater than or equal to the number of SU pairs, then we can expect a good channel allocation number for most of the coalitions. If the number of channels is fewer than the number of SU pairs, they will have to rely on techniques like Time Division Multiple Access to utilize the fewer channels in turn, in consecutive timestamps. However, in the naive scheme, instead of assigning the channels proportionally to the size of coalitions, the channels get assigned equally to the coalitions, irrespective of size.

3.3. Adversarial attack and aversion techniques

In our coalition formation setup, we assume a different set of SUs working together as a coalition with the mal-intent of blocking/starving the legitimate SU pairs of bandwidth, as a result bringing down the utility (in terms of throughput) of the coalition set comprising of the legitimate SU pairs. Our proposed coalitional structure framework can help the legitimate SU pairs by allowing vulnerable SU pairs to make a decision of changing their coalitions such that they are able to utilize the unaffected member sub-channels of another coalition to carry on with their communication, after being blocked. The details of adversarial attack mechanism has been presented in Section 4.3. In Cognisseum, we only consider detecting the presence of adversaries within a channel, detecting the location and other features of the adversaries are out of scope of this work. The coalitions receive the information about adversarial presence from the spectrum sensing mechanism of the existing CRN deployment, as mentioned in Section 3.1

4. Cognisseum: Game-theoretic framework

We propose a coalition formation game for both SU pairs and adversaries in the CRN. The SU pairs work in a joint manner to communicate their channel vacancy information with their peers, so that they can improve their own channel capacities as a coalition.

4.1. Game setup

The Players and Their Goals: From before, let $\mathcal{N} = 1, 2, 3, \ldots, N$ be the set of SUs. The players are $|\mathcal{N}|/2$ SU pairs. Let the players be incorporated into a set $\mathcal{P}$. If there exists a subset S of $\mathcal{P}$, then the subset S is known as 'a coalition'. The goal of the SU pairs is to maximize their channel usage while that of the adversaries is to block as many channels as possible. If channels are blocked, then the SU pairs talking on those channels will also be affected. We design a cooperative hedonic game where the players (SU pairs) may want to join or leave a coalition, or even stay alone.

The Payoff: A function $v(.)$ is used to assign a value to each subset of players, or in other words, to each coalition. If all the members inside the subset S of $\mathcal{P}$ act in unison towards achieving the same goal, then $v(S)$ is the payoff to all members of the coalition. In other words, the value/payoff of the coalition is $v(S)$.

Power Radius: The power radius of each SU pair (a randomly generated positive real number in our case; a constant in reality, unique to a transmitter) means the geographical area that can be covered by each SU pair with its omni-directional antenna range. The transmitter SU of the SU pair is at the center of the said area and the receiver SU can reside anywhere within that area. Here, the blue dots signify the legitimate SU pairs. The lines joining them represent that they can potentially form coalitions, based on their power-radii. The yellow dots represent the malicious users or adversaries.[2] Our assumption of power radius for each of the transmitter and receiver is inspired from the real-world implications of power radii of real devices like a Wi-Fi router. If a router has a higher transmission power, then its power radius will be able to cover an extended area, however, regulatory limits are put in place to limit interference to other neighboring devices. Hence, our algorithm chooses two or mode SU pairs in a potential coalition only if their power radii do not overlap.

Coalition as a Cooperative Game: At the beginning of the game, no coalition exists, hence $v(\phi) = 0$. Based on their common interests, as the members/players start forming coalitions, we have $v(S) > 0, \forall S \subseteq \mathcal{N}$. A detailed discussion in [34] presents the ideas of cooperative game theory. In the characteristic form, an outcome of a game can be as follows: (i) A coalition structure, essentially a partition of $\mathcal{P}$ players into smaller coalitions, and (ii) a payoff vector to distribute

[2] Upon multiple iterations of our experiments, we have come across multiple such cases, where just eyeballing the positions of the SU pairs seems that they are far away from each other, yet they have not taken part in the same coalition. But, in reality, the system-generated random power radius of a particular SU pair might be large enough to render our assumption useless.

the payoff value of each coalition among its members. A non-empty collection of non-empty non-overlapping subsets can be referred to as a coalition structure (CS), $CS = S_1, S_2, S_3, \dots, S_k$ where $S_i \subseteq \mathcal{P}$ represents coalition i and k is the total number of coalitions, which satisfies the followings:

$$\bigcup_{i=1}^{k} S_i = \mathcal{P}; \qquad S_i \cap S_j = \phi \text{ if } i \neq j \tag{1}$$

4.1.1. Stability criteria of coalitions

Two types of stability criteria are considered for our proposed coalitional game: (a) inner and (b) outer. When an SU pair has no incentive to leave its current coalition to become a singleton, then the players (SU pairs) within that coalition have achieved *inner stability*. Similarly, when an SU pair has no incentive to join another coalition, or in other words, no coalition in a CS has any incentive to merge with another coalition, we refer to it as *outer stability*. For example, if we consider a CS with two coalitions S_1 and S_2, then the inner stability conditions will be:

$$v(S_1) > v(i), \forall i \in S_1 \qquad \text{and} \qquad v(S_2) > v(i), \forall i \in S_2 R \tag{2}$$

and the outer stability conditions will be:

$$v(S_2) > v(S_1 \cup S_2) \qquad \text{and} \qquad v(S_1) > v(S_1 \cup S_2) \tag{3}$$

For the rest of the paper, we will express the value function $v(.)$ of joining a coalition as the *payoff function*, quantifying the data rate achieved by joining that coalition. These stability criteria are important metrics as they emerge as useful tools for quantifying the SU pairs' decisions of leaving its current coalition, staying alone or join a new coalition. The game-theoretic stability criteria are well-established and can be found in literature [35]. Later, in Algo. 1, we have exploited stability criteria to decide and come up with a stable coalition set.

4.1.2. Payoff function

Gaussian fading is considered for our proposed framework, for broader applicability. Hence, the wireless transmission parameters are modeled based on Gaussian complex channel. The achievable data rate R in a Gaussian complex channel of bandwidth W is given by the Shannon's information capacity formula [36]:

$$R = W \log_2\left(1 + \frac{P_t G_t G_r \lambda^2}{d^2\ 4\pi N_0 W}\right) \tag{4}$$

where P_t is the transmit power, G_r and G_t are the receive and transmit antenna gains, λ is the wavelength, and d is the distance between the transmitter and receiver within an SU pair. The SU pair's transmitter–receiver channel follows the Friis' transmission equation, and $N_0 W$ is the cumulative noise of that channel. Based on the achievable data rate expression in (4), we can write the payoff or the sum-rate of a singleton i consisting of an SU pair is:

$$R_i = \mu_i W \log_2\left(1 + \frac{P_t^i G_t^i G_r^i \chi}{d_{ii}^2 \mu_i}\right) \tag{5}$$

where $\chi = \frac{\lambda^2}{4\pi N_0 W}$, d_{ii} is the distance between the transmitter and the receiver of the SU pair i, P_t^i is the transmit power of the transmitter of the singleton pair i, G_t^i and G_r^i are the transmit and receive gains for the singleton pair i, and μ_i is the portion of the total bandwidth W allocated to the singleton i. If we represent the channel component as $h_{ii} = \frac{P_t^i G_t^i G_r^i}{d_{ii}^2}$, the sum rate can be re-written as: $R_i = \mu_i W \log_2(1 + h_{ii}\chi/\mu_i)$. Extending this concept for a whole coalition S_c (where we index the SU pairs within coalition S_c with k), we have:

$$R_{S_c} = \mu_{S_c} W \sum_{k \in S_c} \log_2\left(1 + \frac{h_{kk}\chi/\mu_k}{N_0 W \mu_{S_c} + \sum_{j \in S_c, j \neq k} h_{jk}\chi/\mu_{S_c}}\right) \tag{6}$$

where $\sum_{j \in S_c, j \neq k} h_{jk}\chi/\mu_{S_c}$ is the interference received by the receiver of SU pair k from transmitters of all other SU pairs in coalition S_c, $\mu_{S_c} = \sum_{k \in S_c} \mu_k$ is the portion of the bandwidth W being allocated to coalition S_c, h_{kk} represents the channel component for the SU pair k, and h_{jk} represents the channel component between the transmitter of SU pair k and receiver of SU pair k. After the coalition formation algorithm has converged, the set of coalitions will be $CoA = S_1, S_2, S_3, \dots, S_C, \dots, S_\zeta$, where ζ is the total number of formed coalitions. When ζ is less than or equal to the number of sub-channels (C), then all coalitions will get at least one channel. Whereas, if $\zeta > C$ then, there will be at least one coalition which will not get any channel. Therefore, the second case may not converge. Further, ζ or the size of the set CoA should lie between 1 and $|\mathcal{P}|$, i.e., $1 \leq \zeta \leq |\mathcal{P}|$. Naturally, the second case of $\zeta > |\mathcal{P}|$ is unrealistic.

4.2. Coalition formation algorithm

In Algorithm 1, we present the methodology for SU pair coalition formation. The initialization phase of the algorithm includes initializing the initial, intermediate and final coalition sets, PUs and the SU pairs on the plane, randomly initializing the power radii of each SU pair, calculating the Euclidean distance between the given SU pair and other SU pairs, and based on these, forming the potential coalition list. This information is broadcasted over CCC. In most of the cases, the incentive for an SU pair to join the biggest coalition is the highest as there are already more SU pairs in a bigger coalition and more channels are assigned. Then, again, it is imperative that all the SU pairs will judge their own incentive and decide to join the biggest coalition, resulting in a grand coalition.

Ideally, the communication between an SU pair of a coalition should not prevent another SU pair of the coalition from successful communication. This is the reason we decided to introduce the factor of power radius, so that the SU pairs only form an alliance with other pairs who are far enough from each other. This factor results in non-overlapping power radii, which in turn, creates the basis of a healthy communication mechanism. The point to be noted here is that the total combined power radius of an SU pair cannot overlap that of another SU pair. If the combined power radii of two or more SU pairs overlap with each other, then there will be probable communication loss. One could argue that if multiple channels are allocated to a coalition, then in spite of overlapping power radii, different SU pairs could choose different channels and the communication could be carried out successfully. But, we do not always have abundant channels and the proposed algorithm also helps in overcoming the problem of shortage of available channels.

Once initial coalition is formed by checking the *max_pay* value, we then try to evaluate the stability of a coalition k as follows:

(1) Find the maximum payoff *max_pay* of coalition k with all of its members.
(2) If *max_pay* of coalition k is the greatest, then the coalition is already stable.
(3) If *max_pay* of coalition k is the greatest if one SU pair member comes in from coalition j, then the new member is incorporated into k, which then becomes stable.
(4) If the *max_pay* value of the member SU pair of coalition j, alone is greater than that of coalition k itself, then we remove that member from coalition j and put it as a singleton.

These calculations are repeated for all the combinations of coalitions and their members, and the final combination with the maximum *max_pay* value is chosen as the stable coalition(s).

Algorithm 1: Coalition Formation Algorithm

function CoalitionSetFormation($|\mathcal{N}|, W, Q$)
  $\Delta = [\,]$ \ * Initial Coalition Set * \
  $\Theta = [\,]$ \ * Intermediate Coalition Set * \
  $\Omega = [\,]$ \ * Final Coalition Set * \
  $\mathcal{C} \leftarrow W/\mathcal{N}$ \ * Divide W into $\mathcal{N}$ subchannels * \
  while $|\mathcal{N}| \neq \emptyset$ **do**
    Assign SU pairs tx pwr between 0 and 1 Watt.
    Randomly pick SU pair i and SU pair j
    if $tx\ pwr_{SU\ pair_i} \cap tx\ pwr_{SU\ pair_j} = FALSE$ **then**
      InitCoa = {SU pair i ∪ SU pair j}
      Assign $|InitCoa|$ subchannels to InitCoa
      $\Delta \leftarrow$ InitCoa
      $\mathcal{N} \leftarrow \mathcal{N}\backslash$InitCoa}
  while $\Delta \neq \emptyset$ **do**
    Randomly pick SU pair i and SU pair j
    R^i = Achievable rate of SU pair i
    R^j = Achievable rate of SU pair j
    if $R^i < R^i + R^j$ & $R^j < R^i + R^j$ **then**
      $\Theta \leftarrow$ {SU pair i ∪ and SU pair j}
      $\Delta \leftarrow \Delta\backslash$SU pair i ∪ SU pair j}
    else
      $\Theta \leftarrow \Theta\cup$ SU pair i
      $\Theta \leftarrow \Theta\cup$ SU pair j
      $\Delta \leftarrow \Delta\backslash$ SU pair i
      $\Delta \leftarrow \Delta\backslash$ SU pair j
  while $\Theta \neq \emptyset$ **do**
    Randomly pick coalitions x and y
    x = { SU pair i ∪ and SU pair j}
    y = { SU pair k ∪ and SU pair l}
    if $R^x + R^y > R^x$ && $R^x + R^y > R^y$ **then**
      $\Omega \leftarrow \Omega \cup \{x \cup y\}$
      $\Theta \leftarrow \Theta\backslash\{x\}$
      $\Theta \leftarrow \Theta\backslash\{y\}$
    else if $R^x + R^{SU\ pair_k} > R^x$ && $R^x + R^{SU\ pair_k} > R^y$ **then**
      $\Omega \leftarrow \Omega \cup \{x\cup$ SU pair k }
      $\Theta \leftarrow \Theta\backslash\{x\}$
      $\Theta \leftarrow \Theta\backslash\{y\}$
      $\Theta \leftarrow \Theta\backslash$ SU pair k
    else if $R^x + R^{SU\ pair_l} > R^x$ && $R^x + R^{SU\ pair_l} > R^y$ **then**
      $\Omega \leftarrow \Omega \cup \{x\cup$ SU pair l }
      $\Theta \leftarrow \Theta\backslash\{x\}$
      $\Theta \leftarrow \Theta\backslash\{y\}$
      $\Theta \leftarrow \Theta\backslash$ SU pair l
    else
      $\Omega \leftarrow \Omega \cup \{x\}$
      $\Omega \leftarrow \Omega \cup \{y\}$
    return Ω
end function

Algorithm 2: Algorithm for modelling adversarial attack

Inputs: SU pair coalition list (CoA)
Output: SU pair coalition list after adversarial attack (CoA)

/*Phase 1: Initiating the adversaries in the same way as the SU pairs*/
/*Phase 2: Attack strategy*/
if *Smart Strategy:* **then**
  Communicate the potential target list to other adversaries through adversaries' dedicated CCC.
  Attack a SU pair from the potential target list.
  Broadcast the attacked target to other adversaries through CCC such that the other adversaries may remove the already attacked SU pairs from their attack list.
else
  4. Attack a SU pair from the potential target list without updating the other adversaries.
Return the updated coalition list (CoA)

4.3. Adversarial attack model

The adversaries in our case are individual SUs, which are capable of transmitting Additive White Gaussian Noise (AWGN) and in turn disrupting the transmission of one SU pair at a time. The adversaries become successful if they are able to block or jam any SU pair's communication, or in other words, forcing the legitimate SU pairs to adopt a different strategy to keep going on with their transmission. Following the concept of Euclidean geometry, we have calculated the distance between an adversary and any one of the SU pairs. If the power radius of the said adversary overlays (partially or fully) that of the said SU pair, then it is safe to assume that the adversary should be able to block channel used by the SU pair. In Algorithm 2, we show how the adversaries can effectively hamper the stable communication between SU pairs. We propose two types of attack strategies, where adversaries can act either smartly or naïvely rendering to different destructive effect on the proposed framework. In order to ensure that the legitimate SU pairs, especially considering the dynamic and unpredictable nature of adversarial attacks, we make stability checks to confirm the SU pairs' decisions to change their coalitions is optimal and stable. As mentioned in Algo. 1, we perform stability checks after an SU pair leaves its current coalition and, say, decides to join another coalition.

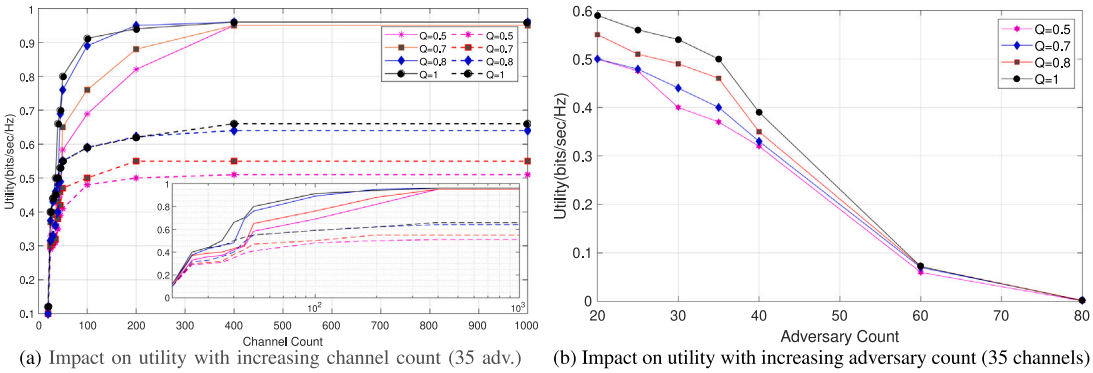
4.4. Preliminary experiments through simulation

We conduct preliminary experiments through simulation to orchestrate the emulation experimental framework. The simulation for the multi-channel, multi-SU-pair and multi-adversary game has been performed under geographical boundary conditions. Since the objective of this paper is to investigate the coalition formation among multiple SU pairs, we set the values of the parameters which reflect the properties of an SU pair as a whole, such as channel gain and interference between two SU pairs. Hence we keep the trivial properties like distance and the antenna gain between the transmitter and receiver of individual SU pairs to unity. There are 50 SU pairs along with 10 PUs in the system. Each of the PUs use their own designated channel. SU pair knowledge of PU activity is according to the Q values. We have used the following parameters for our simulation runs: Bandwidth W = 10 MHz; node deployment area = 100 m^2; transmit power for each node is randomly initialized to a value in (0,1) Watts; and $N_0 = -110$ dBm/Hz. The communication range of each node is set proportional to its transmit power, based on actual IEEE 802.11 g WiFi standard [37]. In our simulations, utility is the total spectral efficiency in bits/sec/Hz of the stable coalition set that we get and it is plotted against various channel and adversary counts (in Fig. 3). We assume a unity channel gain, i.e., $h_{ij} = 1$ for all transmitters $i = 1..100$ and receivers $j = 1..100$. We study how the average utilities of the coalitions vary when we introduce more adversaries into the system keeping the number of SU pairs and channels constant. For each experiment, we run 10 times and then average them out.

4.4.1. Procedure

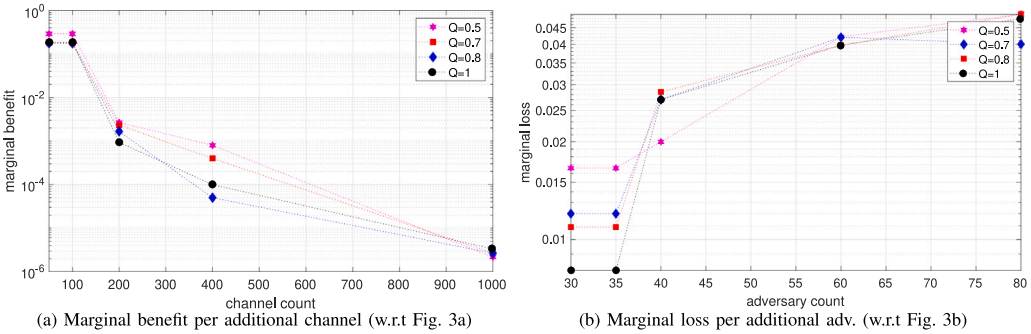
We write the simulation setup in Python 3.10 and run it on a general purpose computer system. Since the main component of our simulation consists of SUs, we take extra care in modeling their game according to the Cognisseum framework, as detailed earlier in this section. We implement the coalition formation algorithm in Algorithm 1 and reinforce the stability criteria of the coalitions. Finally, we introduce the adversarial component into our simulation and implement both the naïve and smart attack strategies by the adversaries. In this process, we vary the Q value and the number of adversaries and channels.

In the following sections, we discuss in detail the insights that we gain after running our simulations.



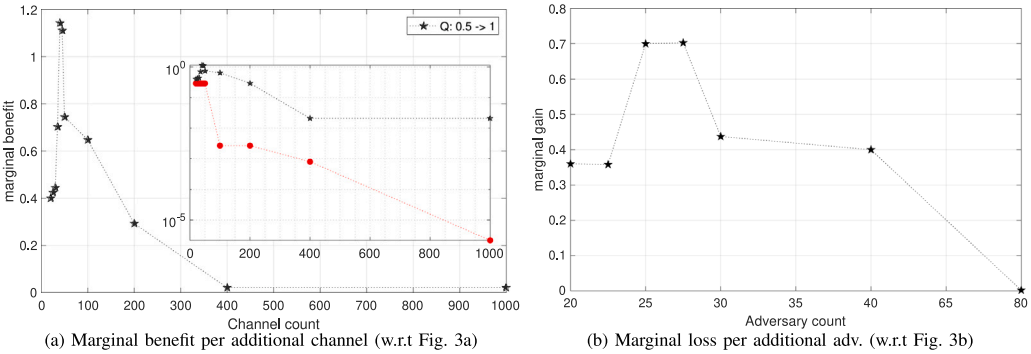
(a) Impact on utility with increasing channel count (35 adv.) (b) Impact on utility with increasing adversary count (35 channels)

Fig. 3. Cognisseum simulation results: Channel and adversary variations. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)



(a) Marginal benefit per additional channel (w.r.t Fig. 3a) (b) Marginal loss per additional adv. (w.r.t Fig. 3b)

Fig. 4. Marginal utility: Additional benefit or loss w.r.t channel and adversary counts, respectively.



(a) Marginal benefit per additional channel (w.r.t Fig. 3a) (b) Marginal loss per additional adv. (w.r.t Fig. 3b)

Fig. 5. Advantage of knowing PU activity: Marginal benefits and losses w.r.t. channel and adversary counts.

4.4.2. *Impact of increasing channel count on utility*

In Fig. 3(a), we show the general increase in utility (in bps/Hz) in each of the coalitions after adversarial attack with respect to the channel count for both smart and naive channel allocation schemes. Here, for various Q values, we have demonstrated the general trend in the increase of the coalitional utility with increasing channel counts. The total number of adversaries is kept constant at 35. For the case when SU pairs have perfect knowledge of PU activity, i.e., $Q = 1$, we see that the utility increases with increasing channel count, but for extremely high channel counts (over 200), the utility saturates and tends to 1 bps/Hz. (For clarity, in Fig. 3, we mention here that the plotted utility values are reported directly without normalization). In the smart channel allocation scheme, when Q is increased from 0.5 to 1, we observe an overall increase in the utility across the range. This behavior is expected because if the SU pairs can predict the PU activities with a higher confidence, their coalitional sum-rate will improve. This set of simulations (in solid lines) show that the aggregate utility of the CRN increases with increasing channel count and then it saturates when the channel counts become large. As we increase the number of channels, we observe that the total utility of the 25 coalitions increases by 160%, on average. This happens because, when under attack, the SU pairs have more leeway to switch to other channels and continue with their communication. In the same plot, we have also shown naive channel allocation scheme using dashed lines that follow the same color scheme as the smart ones. Here, we observe similar pattern with respect to increase in the number of channels as well as the variation in the Q values, however, the utility attained is much lower than that of the smart scheme. This comparison shows that the smart scheme indeed yields a better utility, specifically by about 34.5% than the naive scheme.

4.4.3. Impact of increasing adversary count on utility for the smart channel allocation scheme

In Fig. 3(b), we show the general decrease in utility (in bps/Hz) in each of the SU coalitions after adversarial attack, with respect to the adversary count. Here, for various Q values, we have demonstrated the general trend in the decrease of the coalitional utility with increasing adversary count. The total number of channels is constant at 35. When Q is increased from 0.5 to 1, we observe an overall increase in the utility across the range, due to reasons explained before. This set of simulations show that the aggregate utility of the CRN decreases with increasing adversary count. We infer that the total utility for 25 coalitions decreases with increasing number of adversaries from 20 to 80. As we increase the number of adversaries, we calculate the total utility of the 25 coalitions decreases by about 200%. It is evident that when the number of adversaries deployed becomes large enough, they can render the entire system of CRN useless.

4.4.4. Marginal utility calculation for the smart channel allocation scheme

Now, we focus on the aspect of marginal utility calculation. In Fig. 4(a), we show the marginal benefit in utility per additional channel. In order to calculate this, we consider the percentage improvement in utility per additional channel. For example, when the number of channels is increased from 20 to 50 (in Fig. 3(a)), we calculate the percentage increase in the utility. Then, we divide this percentage increase by the increase in channel count, i.e., $50 - 20 = 30$, in this case. This gives us marginal utility per additional channel. For every Q value, we plot these marginal benefits per additional channel as shown in the figure. We notice that for channel count increment till 50, for every Q value, the marginal benefit is the biggest, so much so to make other benefits negligible. This has been captured in this figure with by switching the y-axis to logarithmic scale. From this figure we conclude that only when the channel count is initially increased from 20 to 50, we see the highest marginal benefit compared to the rest of increment sets.

In Fig. 4(b), we show the marginal loss in utility per additional adversary. In order to calculate this, we consider the percentage deterioration in utility for a set amount of increment in adversary count. For example, when the number of adversaries is increased from 20 to 30 (in Fig. 3(b)), we calculate the corresponding percentage decrement in utility. Then, we divide this percentage decrement amount by the increment in adversary count, i.e., $30 - 20 = 10$, in this case. This gives us additional loss in terms of utility that we suffer per additional adversary. For every Q value, we plot these marginal losses for adversary increments as shown in this figure (y-axis in logarithmic scale). We notice that for every Q value, we see progressively worse marginal benefit or higher marginal loss when adversaries are added.

A key issue is the amount of advantage possible with more knowledge of PU activity. In Fig. 5(a), we show the marginal benefit in utility with higher Q value, shown with the black scatter plot. In order to calculate this, we consider the percentage improvement in utility from $Q = 0.5$ to $Q = 1$. For example, when the Q value is increased from 0.5 to 1 for 100 channels (in Fig. 3(a)), we calculate percentage increase in utility. Then, we divide this percentage increase in utility by the increase in Q values, i.e., $1 - 0.5 = 0.5$. This gives us the marginal benefit in terms of utility that we get with higher Q value. For every channel count we plot these marginal benefits for Q value increment. We notice that for channel count range from 20 to 1000, the marginal benefit increases and then drops down. The highest marginal benefit is observed for 40 channels. Comparing this to Fig. 4(a), for the case $Q = 0.5$, we see the marginal benefits while increasing channel count from 20 to 50 is much less than that seen while increasing the Q values. Not only that, the marginal benefit for $Q = 0.5$ across the range of channel increments (denoted by the dotted red line in the inner plot, with y-axis in logarithmic scale) is lower than that offered by increasing the Q values (denoted by the dotted black line in the inner plot). This enables us to conclude that investing in techniques to improve the SU pair knowledge probability about PU activity in the CRN offers more fruitful outcomes in terms of improving the utility of the coalitions, as compared to investing in increasing the channel count.

In Fig. 5(b), we show the marginal benefit in utility with higher Q value as adversary count varies. In order to calculate this, we consider the percentage increase in utility as Q increases frpm 0.5 to 1. For example, when the Q value is increased from 0.5 to 1 for 30 adversaries (in Fig. 3(b)), we calculate the percentage increase in utility. Then, we divide this percentage increase by the overall increase in Q, i.e., $1-0.5 = 0.5$. This gives us additional benefit in terms of utility that we get per increase in Q. For every adversary count we plot these marginal benefit of knowing more about the PU activity. We notice that for adversary count range from 20 to 80, increasing Q from 0.5 to 1, the marginal benefit increases and then drops down. The highest marginal benefit is observed when there are about 30 adversaries in the system.

Observation 1. *With increasing number of channels, the Cognisseum framework enables better channel utility (see Fig. 3(a)). Also, with decreasing knowledge of PU activities among the SU pairs while increasing channel count, coalitional utility takes a hit (see Fig. 4(a)).*

Observation 2. *With increasing number of adversaries, the Cognisseum framework suffers worse channel utility (see Fig. 3(b)). But, with increasing knowledge of PU activities among the SU pairs while increasing adversary count, coalitional utility actually improves (see Fig. 5(b)).*

Observation 3. *The marginal benefit of increasing the knowledge of the SU pairs about PU activities in the CRN proves to be more when compared to that of just increasing the channel count (see Fig. 5(a)).*

Observation 4. *The marginal loss incurred by increasing the adversary count deteriorates the overall R of the CRN (see Fig. 4(b)).*

4.4.5. Smart vs. naïve attack strategies by the adversaries

The adversaries can choose to be smart or naïve. If they act smart, they should be communicating among themselves through their dedicated CCC and broadcast their SU communication blocking information to others. The potential targets for an adversary are decided by its power radius. Any of the SU pairs falling under that power radius could be chosen by the adversary to block. Now, based on the random geographical position in which all the SU pairs and adversaries are deployed, it could so happen that another adversary might have the same SU pair in its potential blocking list as the previous one. If both of them end up blocking the same one, then they will be wasting their resources and their payoffs as the whole adversarial group will drop. Hence, a smart adversary should always choose an SU pair and communicate its choice to other adversaries (over dedicated CCC), so that they can concentrate on blocking others. In this way, the adversaries as a coalition will be able to wreck a bigger havoc.

On the other hand, adversaries working naïvely without communication will not be able to do as much damage as compared to them working smartly. In Fig. 6, we have compared the normalized utilities of all the 25 formed coalitions with respect to the naïve approach (by taking the utility difference of the two approaches and dividing that with the utility of the naïve approach). In this figure, for various P values, we have plotted the coalitional utility normalized with respect to the naïve attackers. With increasing P values, the normalized utility increases following an exponential curve, denoted by the dotted fit line in the graph. The goodness of fit for this curve is 0.9808. Hence, we conclude that with increasing knowledge of PU activities, smart attack strategy by the adversaries is able to deal exponentially more damage on the CRN.

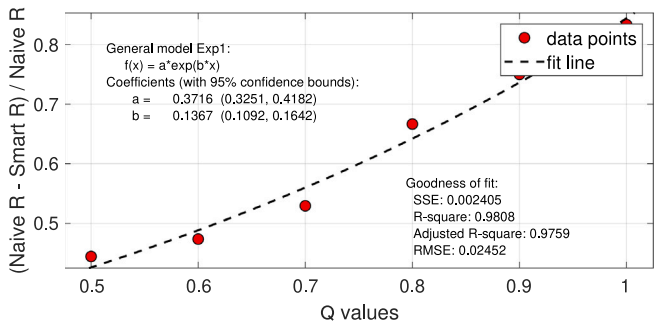


Fig. 6. Cognisseum simulation results: Smart vs. naïve normalization for various Q values.

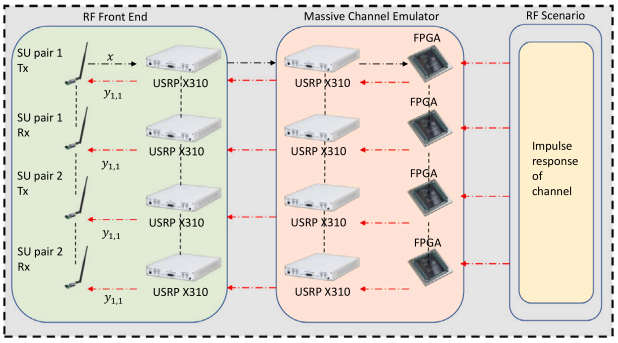


Fig. 7. Colosseum architecture.

4.5. Key takeaways and significance of the presented simulation results:

To summarize the key takeaways, we can say that the utility of SU pair coalitions in Cognisseum increases with the number of channels until it reaches a saturation point, and decreases as the number of adversaries increases. Also, enhanced knowledge of PU activity (higher Q value) significantly boosts utility, with the greatest marginal benefits observed around 40 channels. Adversaries can either act smartly by coordinating to block different SU pairs or naively without communication. Smart adversaries, using their dedicated communication channel, inflict exponentially more damage than their naïve counterparts and this is reflected in the exponential increase in normalized utility with greater adversary knowledge, showing a high goodness of fit of 0.9808.

5. Cognisseum: Hardware emulations on Colosseum

In this section, we discuss how we setup our CRN experiments on the emulation platform Colosseum. We implement the multi-SU-pair multi-attacker CRN concept on Colosseum [11], a large-scale wireless emulator.

5.1. Colosseum wireless emulator

The Colosseum emulator was originally developed to support DARPA's Collaborative Spectrum Challenge [38] and is now a part of the NSF Platform for Advanced Wireless Research (PAWR) [39] program. A detailed description of the Colosseum architecture has been given in [40]. Here, we will discuss some of the important features for the ease of understanding the rest of the discussion.

From a birds-eye view, Colosseum consists of 128 Standard Radio Nodes (SRNs), a Massive Channel Emulator (MCHEM), a Radio Frequency (RF) server, and a management infrastructure. Users can control the SRNs remotely to conduct experiments. Each SRN is a combination of 48-core Intel Xeon server, an NVIDIA Tesla GPU and Ettus USRP X310, operating between 10 MHz and 6 GHz. In Fig. 7, we have shown three blocks: the RF front end, MCHEM, and RF Scenario. The SRNs are part of the RF front end. For our experimentation, we utilize SRNs in multiples of 2 (in accordance with our assumptions stated before). We use two SRNs (a transmitter and a receiver) to create an SU pair. Each of the two SRNs consists of an individual USRP device.

Colosseum has four Internet-facing interactive components as follows [41]:

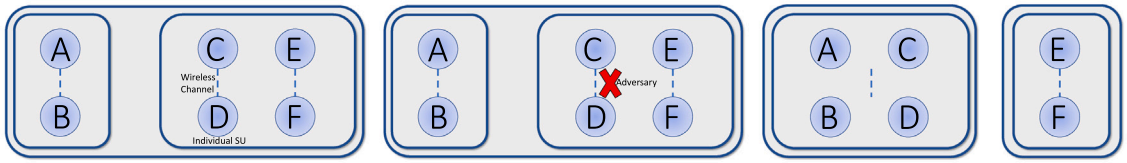
(1) *SSH Gateway*: The gateway address is: '192.10.14.202', which acts as the door for the user to access all of Colosseum's resources.
(2) *User website*: 'https://experiments.colosseum.net': Used for setting up Colosseum resource reservations.
(3) *File-Proxy server*: From the gateway, users can access their Colosseum network storage, including image directory. If a custom SRN image needs to used, it should be uploaded using File-Proxy server.
(4) *SRNs*: These are the actual USRP X310 radio devices which can be allocated to users during their reservations with specific pre-loaded Linux container.

Wireless channel emulation is done by the MCHEM. It contains its own set of 128 USRPs, connected in a one-to-one fashion with those in the RF front end. Apart from the USRPs, MCHEM also contains Field Programmable Gate Array (FPGA) modules which process the digital signals generated by the RF front end. During an RF transmission, the signals generated by the USRPs in the front end get transmitted to the corresponding USRPs in the MCHEM that convert the RF signals to baseband. Finite Impulse Response (FIR) filters on the FPGAs process the signals. The Channel Impulse Response (CIR) between any two SRNs is captured using the 512 FIR filter taps. These channel taps are then applied to signal x through a convolution operation. The effects of the wireless channels are made possible by the scenarios that include path loss and fading. The RF scenario server maintains a catalog of all Colosseum RF scenarios and feeds their channel taps to the channel emulator at run time.

5.2. Hardware-based emulation in Colosseum

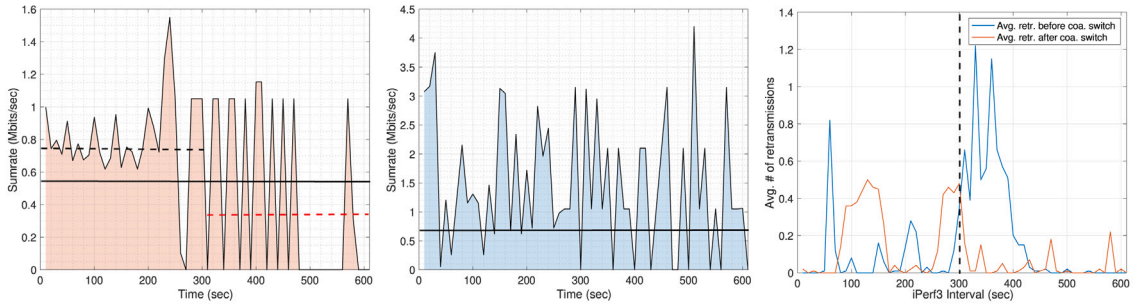
We build up on the software-based approach during emulation on Colosseum. Here, we work with a limited set size of coalitions already formed and assumed to have allocated channels. We achieve this by reserving individual Software-defined Radio Nodes (SRNs) and grouping them in a pairwise basis - a transmitter and a receiver. Coalitions are represented by grouping such pairwise transceivers. The channel conditions of the SRNs are based on [42] and we do not modify them. In order to signify a pair utilizing a sub-channel, we use a channel that has the least amount of permissible pathloss (0 dB pathloss) in Colosseum. In order to signify a coalition having to share its resources (channel(s)) after getting merged with another coalition, we use a channel with higher pathloss. During the experiments on Colosseum, although the radios have a transmit power, we do not consider the power radii of the radios as in the simulation, because we assume the coalitions to be already formed. We start with a predetermined coalition structure and see how the overall network throughput varies for various changes that we make to the coalition structure after introducing the adversaries. As mentioned above, a good channel is one with 0 dB pathloss and increasing the pathloss of a channel makes it progressively worse, making it suitable to use for sub-optimal cases like a coalition having to share its resources.

In the simulation setting, we consider the legitimate SU pairs and adversaries are using different channels and forming coalitions and, at the same time, being attacked by the adversaries. The adversaries, as well, may opt to use a smart or naïve approach as discussed earlier.



(a) Two Coalitions (b) Adv. Attacks the Bigger Coalition (c) Link C-D Switches Coalition

Fig. 8. Representation of emulated CRN in Cognisseum.



(a) R before pair C-D switches coalition (b) R after pair C-D switches coalition (c) Avg. retr. before and after attack

Fig. 9. Cognisseum emulation results. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

5.3. Setting up experimental parameters

Fig. 8 shows the high-level picture of our emulation setup to experiment with the concept of SU coalitions under attack(s) from adversaries (PU presence is assumed but not emulated as our experiments deal with SUs). We start our experiment with a total of six SRNs acting as three SU pairs. Initially, we have two coalitions (see Fig. 8(a)). Nodes A and B communicate with each other over a single channel and they form a single coalition. On the other hand, user pairs C–D and E–F form a bigger coalition; each link gets one channel each. For 300 s, we let this setup continue communicating among themselves. We measure the data rates of individual links and compute the sum rate of all the links for 300 s.

For the hardware emulation, we have chosen 'Test Scenario All Paths 0 dB (1009)' [43] to emulate a perfect channel, as provided by Colosseum and then, for attack emulation, we made the channel progressively worse by using channels with more pathloss. In our setup, initially, all SU pairs use 0 dB path loss channels (using the 0 dB path loss scenario on Colosseum) and we have three channels in total. We use network performance measurement tool `iPerf3` to generate TCP traffic between the transmitters and receivers of the SU pairs. In each of the SU pairs, one acts as the iperf server while the other acts as the iperf client. At 300th second, the adversary joins the network. Unlike the legitimate SU pairs, the adversaries do not work in pairs, rather, they are equipped with a transmitter blasting away AWGN in a specific channel, rendering it useless.

5.4. Emulation results

In this section, we discuss and analyze the results that we get from the emulation part of our Cognisseum framework. Fig. 8(b) illustrates an adversary with a red cross. The adversarial node decides to block channel 2, which is being used by the SU pair C–D. After being attacked, the SU pair C–D has two options: either join the coalition containing A–B or be singleton. For our experimental setup, we have programmed the pair C–D to join A–B. Fig. 8(c) shows the coalition set after C–D joins A–B. Here, A–B and C–D pairs communicate over the same channel and the E–F pair has its own channel. The channel originally used by C–D is now blocked by the adversary. After the coalition switch by C–D, the SU pairs keep communicating for another 300 s. To emulate two links communicating over the same channel, we have chosen a different scenario ID in Colosseum that emulates a channel with 20 dB path-loss. Hence, we use 20 dB path-loss channel for the bigger coalition consisting of the A–B and C–D pairs and the smaller coalition consisting of the E–F pair continues to use a 0 dB path-loss channel.

TCP throughput of the coalition set degrades significantly after the attacker joins. As shown in Fig. 9(a), the dashed black line signifies the sum rate before the adversary attacks the channel used by pair C–D (before the 300 s mark). The dashed red line signifies the sum rate after the attack (after the 300 s mark). The solid black line denotes the overall average sum rate of all the three pairs in the whole duration of 600 s. We have set the `iPerf3` software to record the individual link rate (in Mbits/sec) in intervals of 0.1 s. We have chosen a small interval to better understand how the linkwise rate varies in a sub-second interval when the experiment runs for a long time. Then, we analyze the results after a 10-minute run on Colosseum. During analysis, we take the average of 10 s intervals and plot the results for a total of 600 s. Sum rate of each of the 10-second interval is marked by the individual spikes in the line plot. The final plots are made after averaging several 600-second runs on Colosseum.

Now, we study how the sum rate of the coalition set varies after the link C–D switches coalition. Fig. 9(b) shows the overall sum rate of all the three SU pair after the C–D pair has switched coalition. The data has been collected in the same way as in Fig. 9(b). Here, the solid black line indicates overall sum rate of three SU pairs. Comparing the two figures, we see the overall sum-rate is indeed higher after the SU pair C–D has switched coalition, when compared to that before the switch (marked by the dashed red line in Fig. 9(a)).

We also look into the number of retransmitted packets using `iPerf3`. Fig. 9(c) is about the average number of retransmitted data packets in the TCP protocol used in the `iPerf3` software. Before adversary attack (till the 300 s mark), the average number of retransmissions before the coalition switch is (blue line) shows a lower number. After the adversary attacks the bigger coalition, the total number of retransmissions shoots up, signifying the channel between pair C–D getting blocked. Once the switch is made the plot showing the total retransmissions in orange is overall lower.

Observation 5. *The overall study presented in the emulation corroborates the fact that the adversary can be a deterrent in the ongoing communication*

among legitimate SU pairs in a CRN. Due to the limited number of channel resources present in a coalition, when an additional SU pair joins and starts utilizing the resource of the coalition after being attacked by the adversary, the SU pair is able to attain a higher link capacity and the sum rate of the coalitions improve when compared to that before the SU pair switches to the new coalition (See Figs. 9(a) and 9(b)).

5.5. Key takeaways and significance of the presented emulation results:

The key takeaways and significance of the aforementioned analyses on Colosseum emulator reveal that the sum rate of SU pairs is significantly impacted by coalition dynamics and adversary actions. Before the adversary attack, the sum rate is stable, but it sharply declines after the attack on the C–D channel. However, once the C–D pair switches coalitions, the overall sum rate improves. Additionally, the number of retransmitted packets increases dramatically post-attack, highlighting the disruption caused by the adversary. After switching coalitions, retransmissions decrease, underscoring the effectiveness of coalition restructuring in mitigating adversarial interference. This demonstrates the potential for strategic coalition adjustments to enhance network resilience against attacks.

6. Summary

In this paper, we have devised two distinct approaches as part of Cognisseum: software simulation and hardware-based emulation using the large scale wireless channel emulator called Colosseum.

In the simulation, we showed how SU pairs in an ad-hoc CRN can create coalitions autonomously in the absence of base stations to increase their payoffs. We presented an intelligent coalition formation algorithm and formulated the payoff function for the calculation of the utilities of the SU pairs in terms of throughput/sum rate. We have devised a coalition formation algorithm which can be used by SUs in the CRN to find potential partners for coalition formation. Using these potential coalitions, we have come up with the final coalition model. We also introduced adversaries in the proposed framework and modeled an algorithm for adversarial attack against the legitimate SUs. Next, we presented the data which shows percentage decrease in the average utilities with varying number of adversaries, keeping the number of SUs and channels constant. Then, we showed the increase in coalition utility with increasing number of channels, keeping the number of SUs and number of adversaries as constant along with the difference in coalition utilities for smart and naïve adversarial attack strategies. In the future, we plan to extend this work by comparing our coalition formation and adversarial attack algorithms with the state of the art. Besides, we will also investigate fairness in terms of data rate distribution among the SU pairs.

In the emulation part, we have shown a novel approach towards the calculation of coalitional sum rate before and after adversarial attack using our proposed coalition structure. We have used a variety of channel scenarios to emulate the SU pairs being singleton or part of a coalition. We even modeled a hardware-based adversary and discussed how that hampers communication within a coalition and showed ways by which an SU pair can protect itself by switching coalitions. We have also provided insight into the `iPerf3` software that we have used to record network activity and provided details on packet retransmissions in the TCP framework.

Overall, we believe that this piece of work is the first of its kind to merge a software based simulation solution with the Colosseum platform that models a CRN along with adversarial presence. We envision that this research will serve as a benchmark in the future endeavour of implementing a functioning and complex CRN using Colosseum. Moreover, considering various environment factors within the system modeling and extending it for more number of nodes in Colosseum are our potential future directions.

CRediT authorship contribution statement

Sayanta Seth: Conceptualization, Formal analysis, Investigation, Validation, Writing – original draft, Writing – review & editing. **Debashri Roy:** Supervision, Validation, Writing – original draft, Writing – review & editing. **Murat Yuksel:** Conceptualization, Formal analysis, Funding acquisition, Investigation, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Murat Yuksel reports financial support was provided by National Science Foundation. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation award 2006683.

References

[1] S. Seth, D. Roy, M. Yuksel, Spectrum sharing secondary users in presence of multiple adversaries, in: Network Games, Control and Optimization, Springer International Publishing, Cham, 2021, pp. 125–135.

[2] W. Alhakami, A. Mansour, G. Safdar, Spectrum sharing security and attacks in CRNs: a review, Int. J. Adv. Comput. Sci. Appl. 5 (2014) http://dx.doi.org/10.14569/IJACSA.2014.050111.

[3] D. Niyato, E. Hossain, Competitive spectrum sharing in cognitive radio networks: a dynamic game approach, IEEE Trans. Wireless Commun. (2008) 2651–2660.

[4] V. Valenta, R. Maršálek, G. Baudoin, M. Villegas, M. Suarez, F. Robert, Survey on spectrum utilization in europe: Measurements, analyses and observations, in: 2010 Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2010.

[5] D. Das, S. Das, A survey on spectrum occupancy measurement for cognitive radio, Wirel. Pers. Commun. 2581–2598.

[6] D. Roy, T. Mukherjee, M. Chatterjee, E. Pasiliao, Defense against PUE attacks in DSA networks using GAN based learning, in: IEEE Global Communication Conference, 2019.

[7] J. Yang, H. Zhou, R. Chen, J. Shi, Z. Li, Covert communication against a full-duplex adversary in cognitive radio networks, in: GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 2022, pp. 3144–3149, http://dx.doi.org/10.1109/GLOBECOM48099.2022.10001374.

[8] Z. Xu, Z. Zhang, S. Wang, A. Jolfaei, A.K. Bashir, Y. Yan, S. Mumtaz, Decentralized opportunistic channel access in CRNs using big-data driven learning algorithm, IEEE Trans. Emerg. Top. Comput. Intell. 5 (1) (2021) 57–69, http://dx.doi.org/10.1109/TETCI.2020.3018779.

[9] H.A.B. Salameh, M. Krunz, O. Younis, Cooperative adaptive spectrum sharing in cognitive radio networks, IEEE/ACM Trans. Netw. 18 (4) (2010) 1181–1194.

[10] FCC ET Docket No. 08-260, Second report and order and memorandum opinion and order – unlicensed operation in the TV broadcast bands / additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band, 2008, US Federal Communications Commission, Washington DC, FCC 08-260.

[11] COLOSSEUM The World's Most Powerful Wireless Network Emulator. [Online]. Available: https://www.northeastern.edu/colosseum//.

[12] S. Seth, H. Yazdani, M. Yuksel, A. Vosoughi, Rate-optimizing beamsteering for line-of-sight directional radios with random scheduling, in: 2021 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, 2021, pp. 53–60, http://dx.doi.org/10.1109/DySPAN53946.2021.9677321.

[13] S. Seth, M. Yuksel, A. Vosoughi, Ad-hoc coalition set formation among directional radios, in: 2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems, MASS, 2023, pp. 10–18, http://dx.doi.org/10.1109/MASS58611.2023.00010.

[14] S. Seth, M. Yuksel, A. Vosoughi, Forming coalition sets from directional radios, in: MILCOM 2022 - 2022 IEEE Military Communications Conference, MILCOM, 2022, pp. 507–514, http://dx.doi.org/10.1109/MILCOM55135.2022.10017951.

[15] S. Seth, Coalition Formation and Beamsteering Optimization for Directional Software-Defined Radios (Ph.D. thesis), University of Central Florida, 2023, [Online]. Available: https://stars.library.ucf.edu/etd2023/43/. College of Engineering and Computer Science, Department of Electrical and Computer Engineering.
[16] H. Yazdani, S. Seth, A. Vosoughi, M. Yuksel, Throughput-optimal D2D mmwave communication: Joint coalition formation, power, and beam optimization, in: 2022 IEEE Wireless Communications and Networking Conference, WCNC, 2022, pp. 1539–1544, http://dx.doi.org/10.1109/WCNC51071.2022.9771608.
[17] S. Mustafa, S. Seth, M. Yuksel, M. Rahman, Cellular service with settlement-free peering, in: 2021 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, 2021, pp. 153–162, http://dx.doi.org/10.1109/DySPAN53946.2021.9677342.
[18] A. Baharlouei, B. Jabbari, Dynamic subchannel and power allocation using Nash bargaining game for cognitive radio networks with imperfect PU activity sensing, in: 8th International Conference on Cognitive Radio Oriented Wireless Networks, 2013.
[19] F. Chen, R. Qiu, Centralized and distributed spectrum sensing system models performance analysis based on three users, in: International Conference on Wireless Communications Networking and Mobile Computing, WiCOM, 2010.
[20] X. Xing, T. Jing, W. Cheng, Y. Huo, X. Cheng, T. Znati, Cooperative spectrum prediction in multi-PU multi-SU cognitive radio networks, Mob. Netw. Appl. 19 (4) (2014) 502–511.
[21] L.B. Le, E. Hossain, Resource allocation for spectrum underlay in cognitive radio networks, IEEE Trans. Wireless Commun. (2008) 5306–5315.
[22] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, T. Basar, Coalitional games for distributed collaborative spectrum sensing in cognitive radio networks, in: IEEE INFOCOM 2009, 2009.
[23] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, T. Basar, Coalitional game theory for communication networks, IEEE Signal Process. Mag. (2009) 77–97.
[24] T. Basar, G. Olsder, Dynamic Noncooperative Game Theory: Second Edition, Society for Industrial and Applied Mathematics, 1999.
[25] Yi-Bing, Rui Yang, Fang Ye, Non-cooperative spectrum allocation based on game theory in cognitive radio networks, 2010.
[26] C. Jiang, H. Zhang, Y. Ren, H. Chen, Energy-efficient non-cooperative cognitive radio networks: micro, meso, and macro views, IEEE Commun. Mag. (2014) 14–20.
[27] Z. Han, D. Niyato, W. Saad, T. Başar, A. Hjørungnes, Game Theory in Wireless and Communication Networks: Theory, Models, and Applications, Cambridge University Press, 2012.
[28] Z. Han, K. Liu, Resource Allocation for Wireless Networks: Basics, Techniques, and Applications, Cambridge University Press, 2008.
[29] L. Bonati, P. Johari, M. Polese, S. D'Oro, S. Mohanti, M. Tehrani-Moayyed, D. Villa, S. Shrivastava, C. Tassie, K. Yoder, A. Bagga, P. Patel, V. Petkov, M. Seltser, F. Restuccia, A. Gosain, K.R. Chowdhury, S. Basagni, T. Melodia, Colosseum: Large-scale wireless experimentation through hardware-in-the-loop network emulation, in: 2021 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, IEEE Press, 2021, pp. 105–113, http://dx.doi.org/10.1109/DySPAN53946.2021.9677430.
[30] Tutorial: Colosseum, the World's Largest Wireless Network Emulator. [Online]. Available: https://ece.northeastern.edu/wineslab/papers/melodia2021colosseum_tutorial.pdf.
[31] H. Xu, H. Gao, C. Zhou, R. Duan, X. Zhou, Resource allocation in cognitive radio wireless sensor networks with energy harvesting, Sensors 19 (23) (2019) 5115.
[32] S. Haykin, Cognitive radio: brain-empowered wireless communications, IEEE J. Sel. Areas Commun. 23 (2) (2005) 201–220.
[33] Q. Zhao, B.M. Sadler, A survey of dynamic spectrum access, IEEE Signal Process. Mag. 24 (3) (2007) 79–89.
[34] G. Chalkiadakis, E. Elkind, M. Wooldridge, Cooperative game theory: Basic concepts and computational challenges, IEEE Intell. Syst. (2012).
[35] A. Mas-Colell, M.D. Whinston, J.R. Green, Microeconomic Theory, Oxford University Press, 1995.
[36] A. Goldsmith, Wireless Communications, Cambridge University Press, 2005.
[37] What is the range of a typical wi-fi network? [Online]. Available: https://www.lifewire.com/range-of-typical-wifi-network-816564#:~:text=A%20general%20rule%20of%20thumb,one%2Dthird%20of%20these%20distances.
[38] M. Rosker, Spectrum Collaboration Challenge (SC2) (Archived). [Online]. Available: https://www.darpa.mil/program/spectrum-collaboration-challenge.
[39] Platforms for Advanced Wireless Research. [Online]. Available: https://advancedwireless.org/.
[40] L. Bonati, P. Johari, M. Polese, S. D'Oro, S. Mohanti, M. Tehrani-Moayyed, D. Villa, S. Shrivastava, C. Tassie, K. Yoder, A. Bagga, P. Patel, V. Petkov, M. Seltser, F. Restuccia, A. Gosain, K.R. Chowdhury, S. Basagni, T. Melodia, Colosseum: Large-scale wireless experimentation through hardware-in-the-loop network emulation, in: 2021 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, 2021, pp. 105–113, http://dx.doi.org/10.1109/DySPAN53946.2021.9677430.
[41] Colosseum Architecture. [Online]. Available: https://colosseumneu.freshdesk.com/support/solutions/articles/61000253399-colosseum-architecture//.
[42] KNowledge Base. [Online]. Available: https://colosseumneu.freshdesk.com/support/home.
[43] Northeastern University, Scenario summary list, 2024, https://colosseumneu.freshdesk.com/support/solutions/articles/61000306089-scenario-summary-list. (Accessed 03 June 2024).

Sayanta Seth is an IEEE member and a postdoctoral research fellow at the North Carolina State University. He received his Ph.D. in Electrical Engineering, MS in Electrical Engineering and B.Tech in Electronics and Communications Engineering in 2023, 2018 and 2016 respectively. Prior to joining NC State University, he was a Ph.D. candidate and a a gradaute research assistant at UCF. His research interests are in the area of 5G and beyond wireless communications, mmWave directional antenna beamsteering optimizations, cognitive radio networks, and Open Radio Access Networks (O-RAN). He has published in top IEEE conference proceedings like DySPAN, WCNC, MILCOM and MASS. He has received multiple awards in the form of graduate research support award, multiple graduate presentation fellowships and several IEEE student travel grants. Throughout his career, he has served as chairs for IEEE conferences and has peer reviewed numerous articles published in IEEE transactions and conference proceedings.

Debashri Roy is currently an Assistant Professor at the University of Texas Arlington. Prior to this, she was Associate Research Scientist at the Northeastern University. She received her MS (2018) and Ph.D. (2020) degrees in Computer Science from University of Central Florida, USA. She was an experiential AI postdoctoral fellow at Northeastern University (20202021). Her research interests are in the areas of AI/ML enabled technologies in wireless communication, multimodal data fusion, network orchestration and networked robotics.

Murat Yuksel is a Professor at the ECE Department of the University of Central Florida (UCF), Orlando, FL, and a Visiting Scientist at MIT Lincoln Labs. He served as the Interim Chair of ECE at UCF from 2021 to 2022. Prior to UCF, he was a faculty member at the CSE Department of the University of Nevada, Reno, NV. He received M.S. and Ph.D. degrees in computer science from Rensselaer Polytechnic Institute, Troy, NY in 1999 and 2002, respectively. His research interests are in the areas of networked, wireless, and computer systems with a recent focus on wireless systems, optical wireless, spectrum sharing, network economics, network architectures, and network management. He has been on the editorial boards of Computer Networks, IEEE Transactions on Communications, IEEE Transactions on Machine Learning in Communications and Networking, and IEEE Networking Letters. He has published more than 200 papers at peer-reviewed journals and conferences, and is a co-recipient of five Best Paper, one Best Paper Runner-up, and one Best Demo Awards. He is a senior member of IEEE and ACM.