Spec-GNN: Spectrum Enforcement through Graph Neural Networks in Dynamic Spectrum Access Systems

Chibuikem Ezemaduka, *Graduate Student Member, IEEE,* and Alhussein A. Abouzeid, *Senior Member, IEEE*

***Abstract*—The underlay access mode in dynamic spectrum access (DSA) systems permits secondary users to transmit concurrently with the primary user, provided that the cumulative interference imposed on the primary user does not exceed a set threshold. A spectrum outage is said to have occurred when the interference threshold has been exceeded. To limit the occurrence of an outage, the spectrum sharing policy mandates that all secondary users transmit within set power limits. However, an outage could still occur due to "spectrum violators" who are secondary users that fail to adhere to the spectrum policy, or it could occur due to unforeseen noise within the spectrum environment. In this work, we design an algorithm for detecting and identifying spectrum violators (if any), which we collectively term "enforcement". We propose a novel graph neural network (GNN) based algorithm, Spec-GNN, to identify which secondary users, if any, are spectrum violators when an outage occurs. Because of the noise in a communication system, outages can occur even without the presence of violators, and thus a key challenge is to keep the false alarm rate low. Spec-GNN performs by utilizing as input, a graph of the DSA system formed from data collected from monitoring sensors deployed in the environment. Spec-GNN then learns the roles of each secondary user in the graph, allowing it to classify them as violators or not. We extensively evaluate Spec-GNN across diverse settings with varying number of available sensors, secondary users, and violators. The results show that even with low sensor densities, Spec-GNN can achieve accuracy of around 95% with false alarm rates as low as under 0.03 in realistic outage scenarios. We also show that Spec-GNN's performance is quite robust to the amount of participating secondary users in the DSA system. Even when the number of violators makes up as much as 50% of the secondary users, Spec-GNN is still able to achieve a classification accuracy of close to 92%, while keeping the false alarm rate under 0.04.**

***Index Terms*—Dynamic spectrum sharing, spectrum misuse, power allocation, interference management, deep learning.**

I. Introduction

THE rising demand for additional spectrum and the proliferation of data-intensive applications and devices have accelerated the adoption of technologies like dynamic spectrum access (DSA), which enable more efficient utilization of existing spectrum resources [1], [2]. In DSA systems, various modes are employed to allow secondary users (SU) to access the spectrum while minimizing interference and preventing disruption to the primary user's (PU) operations [3], [4]. In overlay mode, SUs can access the spectrum solely when the PU is inactive in the channel. While this mode offers enhanced protection for the PU, it restricts the average amount of time SUs can utilize the spectrum [5]. Conversely, in the more flexible underlay mode, SUs are permitted to access the spectrum even when the PU is active, provided that the total interference from their transmissions does not surpass a tolerable threshold at the PU [6], [7]. If the interference threshold at the PU is exceeded, this is called an outage [8].

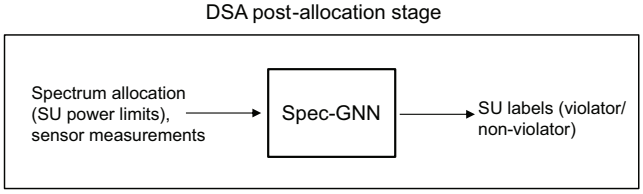


Fig. 1. Basic overview of Spec-GNN's operation.

To prevent an outage, a spectrum manager is typically responsible for allocating spectrum resources, including setting transmission power limits for SUs, to ensure compliance with the PU's interference requirements [9]. When the spectrum manager designates power allocations, it is implicitly assumed that SUs will act in good faith and adhere to their assigned power constraints. However, a significant threat arises if, unbeknownst to the spectrum manager, some selfish or malicious SUs violate their power limits to increase their throughput at the expense of other users or to disrupt the PU's operations [10]. Additionally, malware or device faults could cause SUs to exhibit such behavior. This non-compliant behavior could cause the interference threshold to be exceeded, potentially leading to severe consequences, such as eroding the PU's trust in sharing its spectrum. This could result in the PU opting out of the less restrictive underlay mode or the spectrum-sharing process altogether.

Another potential cause of an outage event is an unexpected change in the wireless environment, resulting in increased noise levels at the PU beyond what the spectrum manager anticipated during the initial power allocation. In such scenarios, an outage may occur even if all SUs strictly comply with their assigned power limits. Therefore, to avoid wrongly accusing innocent SUs in such scenarios, it is crucial that the spectrum manager can accurately distinguish between noise-induced outages and those caused by genuine violators. Correctly identifying guilty SUs only in cases of actual violations prevents unfairly penalizing compliant SUs and ensures the integrity and fairness of the spectrum enforcement process.

The objective of this work is to devise a novel method to accurately identify spectrum violators in the event of an outage within an underlay DSA system. Our work specifically addresses the post-allocation stage, where the spectrum

This material is based upon work supported by the U.S. National Science Foundation under Award No. 2007454.

The authors are with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY 12180 USA (email:ezemac@rpi.edu; abouzeid@ecse.rpi.edu).

TABLE I
KEY DIFFERENCES BETWEEN RECENT ENFORCEMENT APPROACHES AND SPEC-GNN

Category	**Prior Works** [11]–[14]	**Spec-GNN**
DSA mode	Overlay	Underlay
Violator type	SUs with unauthorized access (intruders)	Authorized SUs exceeding assigned power limits
ML approach	CNN based	GNN based
Outage classification	No distinction between noise-induced and violation-induced outages	Differentiates between noise-induced and violation-induced outages

manager seeks to detect whether SUs comply with their previously assigned power limits, and if not, correctly identify the violators. We do not consider the allocation process itself, but rather this work complements existing allocation strategies through effectively identifying violators, as shown in Fig. 1. To achieve this goal, we propose a deep learning approach based on a graph neural network (GNN), named Spec-GNN, which identifies any secondary users exceeding their allocated power levels when an outage is observed. We assume that although the spectrum manager knows the allocated power limits for each SU, it lacks direct information regarding the exact transmit powers utilized by the SUs during operation. It is important to point out that some other studies (discussed in Section II) have focused on identifying spectrum offenders in the less complicated overlay mode, where SUs are totally prohibited from transmitting when the PU is active. However, to the best of our knowledge, our work is the first to address the challenge of identifying spectrum violators in the more challenging underlay mode, where SUs are allowed to transmit together with the PU.

Spec-GNN is designed to identify spectrum violators whenever an outage occurs. Due to the noise in the system, we categorize outages in underlay DSA systems into three categories, which Spec-GNN aims to identify. Spec-GNN leverages the data collected from crowdsourced sensors to construct a graph representation of the environment during an outage event. Spec-GNN utilizes this graph along with learned graph features to identify specific SUs, if any, responsible for causing the outage. We comprehensively evaluate Spec-GNN's performance across multiple simulated outage scenarios and validate its effectiveness through extensive experimental results.

The remainder of the paper is organized as follows. Section II provides an overview of the related literature, while Section III formally defines our problem and its context. We describe our proposed solution in Sections IV and IV-A, followed by an evaluation in Section V. Section VI concludes the paper by highlighting possible future avenues for research.

II. RELATED WORKS

Enforcement of spectrum policy in dynamic spectrum sharing can be broadly categorized into two approaches: *ex ante* methods, which aim to prevent or minimize the likelihood of spectrum misuse, and *ex post* methods, which involve detecting instances of policy violation and applying appropriate penalties [15]. While *ex ante* approaches are effective in regulating access to shared spectrum and preemptively safeguarding the PU, they inherently rely on the assumption that SUs will act in accordance with the established rules, which may not always be the case. On the other hand, *ex post* methods acknowledge the possibility that not all SUs will comply with regulations, necessitating the identification and prevention of violators, to mitigate disruptions to the PU's operations.

Several studies have explored various aspects of *ex post* enforcement. For instance, in [16], the authors introduce a framework aimed at detecting and penalizing spectrum misuse to discourage future violations in spectrum sharing systems. Meanwhile, [10] proposes and evaluates a crowd-sourced spectrum monitoring framework as a cost-effective alternative to dedicated monitors, addressing detection of spectrum violations. Similarly, [17] explores using crowd-sourced measurements to optimally schedule mobile autonomous agents to enhance enforcement accuracy. Recognizing concerns about sensor untrustworthiness, [18] leverages blockchain networks to enhance enforcement reliability. Additionally, the authors in [19] focus on selecting trustworthy crowd-sourced volunteers, while the work in [20] formulates spectrum monitoring as a combinatorial adversarial multi-armed bandit problem to efficiently utilize limited resources. Furthermore, [21] addresses spectrum misuse detection alongside sensing for spectrum holes via multi-hypothesis testing.

Other studies emphasize real-time transmitter identification to detect unauthorized spectrum access. Works such as [22]–[26] propose embedded spectrum permits or waveform authentication to identify transmitters in shared spectrum systems. However, implementing spectrum permits and transmitter authentication introduces additional overhead and costs, necessitating collaboration with equipment manufacturers for seamless integration.

To circumvent such complexities, recent works [11]–[13] have explored cost-effective algorithms utilizing received signal strength (RSS) measurements from commodity crowd-sourced sensors, to detect and localize spectrum violations in shared spectrum environments. For instance, [11] employs a maximum a posteriori approach for localizing unauthorized SUs. Meanwhile, [13] addresses the same issue with a deep learning approach that treats the problem as an image-to-image translation task, employing convolutional neural networks (CNNs) for localization. Similarly, A deep learning strategy is proposed in [12] to localize violators while minimizing the data required to train their CNN model. In addition, the authors

TABLE II
TABLE OF NOTATIONS

Notation	Description	Notation	Description
p_i	i^{th} SU's allocated transmit power limit	$\mathcal{V}_U$	Set of SU nodes
$\tilde{p}_i$	i^{th} SU's actual transmit power unknown to the spectrum manager	$\mathcal{V}_S$	Set of sensor nodes
T	PU interference threshold	e_{ij}	Edge between the i^{th} SU node and j^{th} sensor node
$\tilde{T}$	Actual interference observed by the PU	a_v	v^{th} sensor node's measured power
d	Difference between the actual interference observed by the PU and its threshold; d = $\tilde{T}$ - T	$\mathcal{N}(v)$	v^{th} node's neighborhood
g_i	Channel gain between the i^{th} SU and PU	h_v^l	v^{th} node's representation at the l^{th} layer of the GNN model
n	Unknown noise present at the PU during the SU transmissions	$\hat{n}$	Spectrum manager's estimate of n

in [14] employ generative adversarial networks (GANs) to localize violators while preserving PU privacy.

Despite these advancements, the majority of existing works address spectrum violations characterized by unauthorized SUs transmitting in prohibited channels (overlay DSA). These techniques are specialized for detecting intruders within the spectrum area, and do not readily generalize to the underlay mode, where authorized SUs coexist with the PU, constrained by specified interference thresholds. In underlay scenarios, violators are authorized SUs that exceed their allocated power limits, leading to a spectrum outage if the interference threshold is surpassed.

Our work thus differs from others as we uniquely address the problem of identifying violators during outages specifically in underlay DSA systems, which to the best of our knowledge, has not been previously addressed. While related work such as [27] proposes fairness-driven spectrum allocation based on SUs' historical compliance, it broadly assumes the availability of compliance data without detailing its acquisition or real-time violation identification. In this work however, we propose a novel and practical method to identify any SUs that violate spectrum allocations in real-time. Building on the recent successes of deep learning in wireless communications [28], we address this challenge by designing a GNN based algorithm, Spec-GNN, which is capable of managing uncertainties such as dynamic wireless conditions and unpredictable number of violators. Table I summarizes our novel contributions relative to existing enforcement literature.

Finally, we acknowledge that several works [29]–[37] have investigated efficient resource allocation strategies in underlay DSA systems. However, such allocation-focused approaches fall beyond the scope of our work, which is solely concerned with *ex post* enforcement following resource allocation.

III. PROBLEM FORMULATION

Consider a DSA system overseen by a spectrum manager responsible for regulating secondary users' access to the shared spectrum. In this system, the manager authorizes SUs to transmit concurrently with the primary user of the band. However, the PU imposes a stringent requirement for sharing its spectrum: the total interference power from external sources to the PU's system must not exceed a specified threshold to prevent disruption to its operations. Let T represent this interference threshold (which can for example be communicated by the PU to the spectrum manager), define the maximum interference the PU can tolerate[1]. To satisfy the PU's requirement, the spectrum manager assigns a maximum transmit power limit to each SU authorized to access the spectrum, ensuring that the total interference does not exceed T. Let p_i denote the power limit allocated by the spectrum manager to the ith SU among K SUs such that:

$$\sum_{i=1}^{K} p_i g_i + \hat{n} \leq T, \tag{1}$$

where g_i represents the known channel gain for the ith SU's transmission path to the PU, and $\hat{n}$ denotes the spectrum manager's estimate of n, the environmental noise present at the PU during the SUs' transmissions. n could exceed $\hat{n}$ during the system's operation due to the presence of unexpected noise arising from unforeseen transmissions from unknown sources in the spectrum area or general unpredictability of the wireless environment[2]. Once the ith SU receives its power allocation, let $\tilde{p}_i$ denote the actual transmit power used by the SU, which is unknown to the spectrum manager. During SU transmissions, let the actual interference observed by the PU, which it constantly reports to the manager, be denoted by $\tilde{T}$. Thus,

$$\sum_{i=1}^{K} \tilde{p}_i g_i + n = \tilde{T}. \tag{2}$$

Let $d = \tilde{T} - T$ denote the difference between the actual interference observed by the PU and the interference threshold. Therefore from (1) and (2),

[1]We assume that before specifying T, the PU has sufficient knowledge of its system's internal noise sources, which are already accounted for. Therefore, T is set solely to limit external interference and does not include internal receiver noise such as thermal noise.

[2]To mitigate the impact of such potential deviations between $\hat{n}$ and n, the spectrum manager may choose to adopt conservative power allocation strategies so as to ensure that T would still not be exceeded. As discussed in Section II, efficient resource allocation methods have been treated extensively and are beyond the scope of this work.

$$d \leq \sum_{i=1}^{K} \tilde{p}_i g_i + n - \sum_{i=1}^{K} p_i g_i + \hat{n} \tag{3}$$

$$d \leq \left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) + \left(n - \hat{n} \right). \tag{4}$$

The spectrum manager identifies an outage when, at any point in time, $d > 0$, indicating that the actual interference observed at the PU exceeds its maximum tolerable level. This condition $d > 0$ can occur under the following circumstances:

1) Type A: When $\left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) \leq 0$ and $(n - \hat{n}) > 0$ where $| \left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) | < (n - \hat{n})$, i.e., although the total power received at the PU from the SUs' transmissions does not exceed the expected limit, an outage occurs due to additional unpredicted noise at the PU. This outage event is not caused by spectrum violators.

2) Type B: When $\left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) > 0$ and $(n - \hat{n}) \leq 0$ where $\left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) > |n - \hat{n}|$. This scenario indicates that although the actual noise at the PU does not exceed the manager's estimate, the outage is caused by at least one SU transmitting above its power limit, resulting in the total power received at the PU from the SUs' transmissions exceeding the expected limit. Clearly, if $\left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) > 0$, then $\tilde{p}_i - p_i > 0$ for at least one SU i. In such cases, any SU i for which $\tilde{p}_i - p_i > 0$, is termed a spectrum violator. This case is an outage event caused solely by spectrum violation.

3) Type C: When $\left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) > 0$ and $(n - \hat{n}) > 0$, the outage occurs due to a combination of spectrum violators transmitting above their allocated power limits, and unforeseen environmental noise at the PU.

The aforementioned outage cases are referred to as Type A, Type B, and Type C outages respectively. Upon detecting an outage, the spectrum manager's goal is to identify spectrum violators among the SUs, if any. Subsequently, appropriate corrective actions, outside the scope of this work, may be implemented to address the outage depending on its identified origin. It is important to note that there are conditions where spectrum violators may exist, or unforeseen noise may be present at the PU, yet no outage is observed. For instance, consider a variation of the Type A scenario where some spectrum violators exist, but their excess transmission power is balanced by other non-violators who transmit below their assigned limits by an equal or greater amount, resulting in $\left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right)$ remaining non-positive. In such cases, if $(n - \hat{n}) \leq | \left(\sum_{i=1}^{K} \left(\tilde{p}_i - p_i \right) g_i \right) |$, the spectrum manager does not observe an outage since the interference received at the PU does not exceed the threshold. In this paper, we generally do not consider identifying the violators for any such case where $d \leq 0$, as these situations do not impede the PU's operations. We assume the spectrum manager is interested in a cost-effective approach of enforcing spectrum policy only when an outage has been identified $(d > 0)$.

It is also important to emphasize that this work focuses solely on the violator identification stage following a spectrum outage, and not on the design of resource allocation or noise estimation mechanisms. The allocated transmit powers p_i and noise estimate $\hat{n}$ are assumed to be provided by the spectrum manager based on any suitable ex ante strategies [29]–[37]. The actual values $\tilde{p}_i$ and n are unknown and not directly observable, and are inferred indirectly through interference measurements and sensor data. In the next section, we outline our proposed solution to achieve the system's objectives.

IV. Graph based framework for Identifying Spectrum Violators

To achieve the objective described in Section III, we introduce a graph-based method that we believe aligns well with the nature of the problem. Initially, upon detecting an outage, the spectrum manager tasks monitoring sensors with surveying the spectrum sharing area. These sensors gather information about the spectrum environment in the form of received power measurements, capturing both the transmissions of SUs and environmental noise. A cost-effective strategy involves leveraging crowd-sourced low-commodity sensors, which has become a favored approach in recent spectrum monitoring efforts [10], [38], [39]. Using the received sensor measurements and known channel gains between sensors and SUs, the spectrum manager constructs a bipartite graph $\mathcal{G}\left(\mathcal{V}_U, \mathcal{V}_S, \mathcal{E}\right)$ representing the spectrum environment. Here, the two disjoint sets of nodes, $\mathcal{V}_U$ and $\mathcal{V}_S$, represent the SUs and deployed sensors respectively, with edges connecting every SU-sensor pair. The value of an edge $e_{ij} \in \mathcal{E}$ between the ith SU node and jth sensor node, corresponds to the channel gain between them. The problem then naturally translates into a node classification task where the objective is to classify each SU node as either a violator or non-violator, a task addressed using Spec-GNN, as detailed subsequently[3].

A. Classifying SU Nodes with Spec-GNN

Next, we provide details on Spec-GNN, our solution to the node classification problem. GNNs represent cutting-edge deep learning models tailored for graph-centric tasks and have demonstrated significant success in node classification [40]. Employing a message passing scheme, GNNs effectively capture intricate relationships and dependencies among nodes within a graph. They accomplish this by propagating each

[3]Following classification of each SU node, if no nodes are identified as violators, the outage can be attributed to being caused solely by unexpected noise at the PU (Type A outage). However, if at least one SU node is classified as a violator, then the outage is attributed as either Type B or Type C. To specifically determine if it is a Type B or Type C outage, the manager could first decide to implement corrective measures to mitigate the impact of the already identified violators, such as revoking their spectrum access. Detailed investigation into effective corrective measures remains a subject for future work. If the manager no longer observes a violation after those measures, it can conclude that the initial outage was Type B. However, if the outage still persists, it concludes that the initial outage was Type C, resulting from both violators and unexpected external noise at the PU.

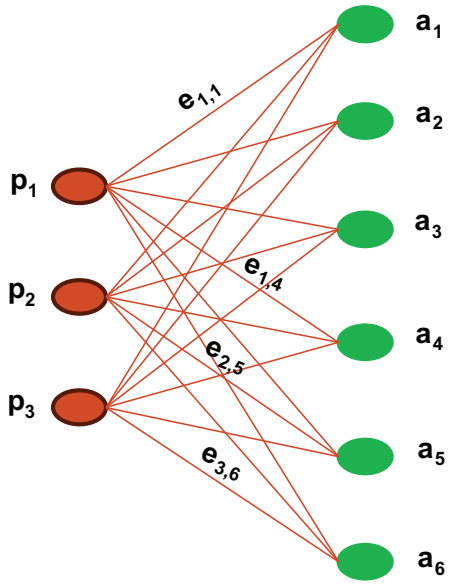


Fig. 2. Example of a bipartite graph representation for a scenario involving 3 SUs and 6 sensors in the spectrum area. Each SU node i is characterized by its assigned power, p_i, while each sensor node j is represented by its measured power, a_j. Edge weight $e_{i,j}$ denotes the channel gain between the respective SU and sensor nodes.

Algorithm 1: Spec-GNN

input : Graph $\mathcal{G}(\mathcal{V}_U, \mathcal{V}_S, \mathcal{E})$; Assigned power limits $p_v, \forall v \in \mathcal{V}_U$; Measured powers $a_v, \forall v \in \mathcal{V}_S$; edge weights $e_{u,v}, \forall v \in \{\mathcal{V}_U \cup \mathcal{V}_S\}$ and $\forall u \in \mathcal{N}(v)$; model depth L; Weight matrices $\mathbf{W}^l_{1,\mathcal{V}_U}, \mathbf{W}^l_{2,\mathcal{V}_U}, \mathbf{W}^l_{1,\mathcal{V}_S}, \mathbf{W}^l_{2,\mathcal{V}_S}, \forall l \in \{1, ..., L\}$; activation function σ; MLP classifier function MLP

output: SU class $\mathbf{b}_v, \forall v \in \mathcal{V}_U$

$\mathbf{h}^0_v \leftarrow p_v, \forall v \in \mathcal{V}_U$;
$\mathbf{h}^0_v \leftarrow a_v, \forall v \in \mathcal{V}_S$;
for $l = 1, ..., L$ **do**
  for $v \in \mathcal{V}_U$ **do**
    $\mathbf{h}^l_v \leftarrow \sigma\left(\mathbf{W}^l_{1,\mathcal{V}_U}\mathbf{h}^{l-1}_v + \mathbf{W}^l_{2,V_U}\sum_{u\in\mathcal{N}(v)} e_{u,v}\mathbf{h}^{l-1}_u\right)$
  end
  for $v \in \mathcal{V}_S$ **do**
    $\mathbf{h}^l_v \leftarrow \sigma\left(\mathbf{W}^l_{1,\mathcal{V}_S}\mathbf{h}^{l-1}_v + \mathbf{W}^l_{2,\mathcal{V}_S}\sum_{u\in\mathcal{N}(v)} e_{u,v}\mathbf{h}^{l-1}_u\right)$
  end
  $\mathbf{h}^l_v \leftarrow \mathbf{h}^l_v / \|\mathbf{h}^l_v\|_2, \forall v \in \{\mathcal{V}_U \cup \mathcal{V}_S\}$
end
$\mathbf{b}_v \leftarrow MLP(\mathbf{h}^L_v), \forall v \in \mathcal{V}_U$;

node's local neighborhood information across multiple network layers, enabling the model to acquire comprehensive insights into the graph's structure and attributes, essential for solving specific tasks. In node classification tasks, GNN models learn for each node, a vector representation that encapsulates latent information about the global graph structure, and relationship with other nodes. This vector can subsequently be inputted into a multi-layer perceptron (MLP) to determine the node's class. Another compelling rationale for employing GNNs in our context is the dynamic nature of the DSA system, where the number of SUs requiring spectrum access and the deployment of crowd-sourced sensors, can vary over time based on availability. Therefore, the spectrum manager's graph could have an unpredictable number of nodes and edges at any given attempt to identify violators. Training distinct models for all potential permutations of SUs and sensor locations would be both impractical and costly. To address this challenge effectively, neural network architectures like GNNs offer a practical solution by enabling training and inference on input data of variable size, a capability not easily achievable with classical models such as convolutional neural networks. We therefore propose Spec-GNN, a GNN algorithm inspired by GraphSAGE [41] which excels at learning inductively and generalizing well to unseen nodes and graphs not present in the training data. This capability is well-suited for our scenario, where the spectrum environment is dynamic and unpredictable. However, GraphSAGE is not applicable to our problem in its vanilla form as it does not consider edge weights, and disjoint node sets having distinct features. Thus, to better align with our objectives, Spec-GNN adopts key modifications to GraphSAGE's forward propagation algorithm, as outlined shortly. By incorporating the initial features of each SU node and its neighbors, Spec-GNN learns a low-dimensional embedding that captures the structural information about each node's role in the graph. This learned representation for an SU node is subsequently fed into an MLP to determine the SU's class. Spec-GNN's update rule for any node v of type c, where c can be either $\mathcal{V}_U$ or $\mathcal{V}_S$, is as follows:

$$\mathbf{h}^l_v = \sigma\left(\mathbf{W}^l_{1,c}\mathbf{h}^{l-1}_v + \mathbf{W}^l_{2,c}\sum_{u\in\mathcal{N}(v)} e_{u,v}\mathbf{h}^{l-1}_u\right) \forall l = 1...L, \tag{5}$$

where $\mathbf{h}^l_v$ denotes the node's representation at the lth layer of the model, and $\mathbf{W}^l_{1,c}$ and $\mathbf{W}^l_{2,c}$ represent the lth layer's weight matrices specific to node type c. $\mathbf{W}^l_{1,c}$ transforms the node's representation from the previous layer, while $\mathbf{W}^l_{2,c}$ transforms the aggregation of the neighbors' information from the previous layer. $\mathcal{N}(v)$ denotes the node's neighborhood, and $e_{u,v}$ represents the weight of the edge between the node and its uth neighbor, which as mentioned earlier, corresponds to the channel gain between them. σ is the activation function used to introduce non-linearity during the node updates. $\mathbf{h}^0_v$ represents the node's initial input feature, which depends on the node type: for an SU node, $\mathbf{h}^0_v = p_v$, while for a sensor node, $\mathbf{h}^0_v = a_v$, where a_v is the sensor's measured power. Fig. 2 illustrates an example of a graph sample fed into Spec-GNN. Due to the disparate feature types between the two node sets, we segregate the layer transformation weights based on their respective categories. This approach allows Spec-GNN to focus on learning latent information specific to each node set. For the sensor nodes, Spec-GNN learns information about any

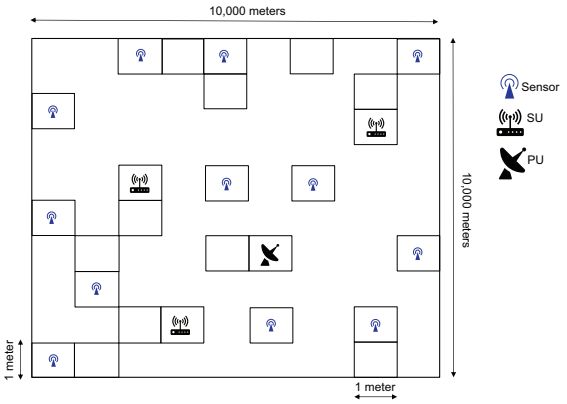


Fig. 3. Random placement of a PU, SUs, and some sensors within the simulation area.

present sub-violations due to learned deviations between each sensor's actual and expected measured power. Meanwhile for the SU nodes, through multi-layer message passing, their final representations contain complex information on the relative role that they contribute to the sub-violations, in addition to information on the latent relationships between themselves and with the sensor nodes. We also integrate edge weights into Spec-GNN to ensure that spatial relationships between nodes influence the learning process effectively. Spec-GNN's algorithm for identifying violators is delineated in Algorithm 1.

Spec-GNN aligns with the fundamental objective of underlay DSA systems: to maximize the performance of SUs while ensuring that interference to the PU remains within acceptable limits. Rather than altering the initial resource allocation or power control strategies, Spec-GNN functions as a complementary reactive mechanism. In instances where an outage occurs, Spec-GNN empowers the spectrum manager to identify and isolate non-compliant SUs whose transmissions violate the PU's interference constraints. This post-allocation stage is essential for upholding interference guarantees that are critical to PU protection and the sustainability of underlay spectrum sharing. Moreover, violations not only degrade PU performance but can also destabilize the system by disrupting prior power allocations and introducing interference to other SUs. This degrades overall network efficiency and fairness. By accurately identifying violators, Spec-GNN enables potential corrective actions such as revoking access, thereby restoring the system's intended equilibrium: safeguarding the PU while maximizing throughput for compliant SUs.

In the following section, we detail Spec-GNN's training process and experimental setup for its evaluation, followed by a presentation of evaluation results.

V. Evaluation

We perform python-based simulations within a 10 km x 10 km spectrum-sharing environment subdivided into 1 m x 1 m grid cells. In our setup, the PU, SUs, and crowd-sourced sensors are randomly positioned at the centers of these grid cells, as illustrated in Fig. 3. Our evaluation assesses Spec-GNN across various outage scenarios, and we analyze the results using pertinent metrics[4]. In the following section, we provide a detailed description of the procedures for generating the training and test data, as well as for training the model. We will then outline the metrics employed for evaluation and present the resulting outcomes.

A. Data Generation and Model Training

To capture the dynamic nature of the enforcement process, our training and test datasets feature graphs of varying sizes, where each graph sample has a random number of SUs ranging from 2 to 10, and between 20 to 1000 sensor nodes (0.00002% to 0.001% sensor density). Without loss of generality, edge weights between nodes in the graph are calculated using the simple free space propagation model (inverse of the square distance between nodes). The datasets consist of samples designed to represent all three outage types. The power limits assigned by the spectrum manager to the SU nodes ranges from 0.1 to 10 Watts (20 to 40 dBm). For configurations corresponding to Type A outages, scenarios are simulated where no SU node exceeds its allocated power limit, and all SUs are categorized as non-violators. In these scenarios, unforeseen noise sources are introduced, which may include a randomly positioned unauthorized transmitter in the vicinity, noise sampled from a uniform distribution, or a combination of both. The choice of unexpected noise source for each sample is randomly chosen from those options. For Type B outage scenarios, where no unexpected noise is present, a subset of SUs is randomly labeled as violators, transmitting between 0.1 and 10 Watts above their assigned limit. In Type C outage scenarios, the samples incorporate both unexpected noise sources and labeled violators. We streamline the simulations by configuring the SUs to transmit at or above their maximum permitted power, depending on the outage scenario, and by assuming that the actual environmental noise meets or exceeds the spectrum manager's estimate. As described in Section IV-A, each SU node's input feature is its assigned power limit, while each sensor node's feature is its measured power. Prior to training, we enhance the model's learning efficiency by subtracting the known received power due to the PU's transmission, and the spectrum manager's noise estimate, from the sensors' measurements. This adjustment ensures that the input sensor power solely reflects the unknown transmissions from SUs and any unexpected noise in the environment. Furthermore, to accelerate convergence during training, we preprocess the edge weights by scaling them by a factor of 10^4, ensuring they are on the same magnitude scale as the node features. Our model is trained in a supervised manner, where violators and non-violators are labeled with class values of 1 and 0, respectively. The GNN, coupled with the MLP, is trained end-to-end using the binary cross-entropy loss function and the Adam optimizer. Our MLP consists of a single hidden layer with 400 neurons. After experimenting with various configurations on our validation set, we finalize our training hyperparameters as follows: We set the GNN depth to $L = 4$,

[4]We do not evaluate Spec-GNN against any prior work in literature because, to the best of our knowledge, our work is the first to tackle the problem of identifying violators in underlay DSA systems.

and use the rectified linear unit (ReLU) activation function for all layers except the output layer of the MLP, where we apply the sigmoid function. We determine that a node embedding dimension of 128 yields optimal performance; other dimensions did not improve results significantly. Our implementation utilizes the PyTorch Geometric (PyG) library on an Intel core i7 2.6 GHz PC having 8 GB Nvidia Geforce RTX GPU and 32 GB RAM. We train the model using a total of 30,000 samples, which include 10,000 samples per outage type. During training, we employ a batch size of 128, a learning rate of 0.001, and train for 1000 epochs.

Although for clarity and tractability, our current formulation assumes a fixed interference threshold T within each simulation sample, Spec-GNN may be extended to operate under dynamic interference constraints driven by channel state information (CSI). In such settings, sensors would monitor RSS across different coherence intervals, reflecting the PU's varying interference tolerance. Spec-GNN can then be applied independently on a per-interval basis, restricted to those intervals in which the interference threshold is exceeded. For each such interval, the input graph would be constructed using RSS measurements from sensors active during that interval, along with the assigned SU power limits. Spec-GNN would then perform node classification relative to the threshold applicable in that specific coherence window. This design preserves Spec-GNN's enforcement capability while leveraging its inductive generalization over varying graph structures. Related works on CSI-driven dynamic threshold adaptation include [42], [43] which may guide future extensions that couple dynamic allocation and enforcement. A formal consideration and evaluation of such per-interval enforcement under dynamic interference thresholds, is left to future work.

B. Evaluation metrics

We assess Spec-GNN's performance with the following standard metrics

1) SU Classification accuracy: This defines the model's accuracy in classifying each SU as either a violator or non-violator. It is expressed as

$$\text{Accuracy} = \frac{\text{Number of correctly classified SUs}}{\text{Total number of SUs}}. \quad (6)$$

2) F1 Score: Let TP, FP, and FN denote the number of True Positives, False Positives, and False Negatives respectively. Recall (also known as Detection Rate) is defined as $\frac{TP}{TP+FN}$ while Precision is given by $\frac{TP}{TP+FP}$. The F1 Score, which balances Precision and Recall, is calculated as

$$\text{F1 Score} = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}. \quad (7)$$

3) False Alarm Rate (FAR): This represents the proportion of non-violators that are incorrectly classified as violators. It is defined as

$$\text{FAR} = \frac{FP}{FP + TN}. \quad (8)$$

4) Cardinality Error: This refers to the proportion of instances where the estimated number of violators differs from the actual number of violators [44]. It is defined as

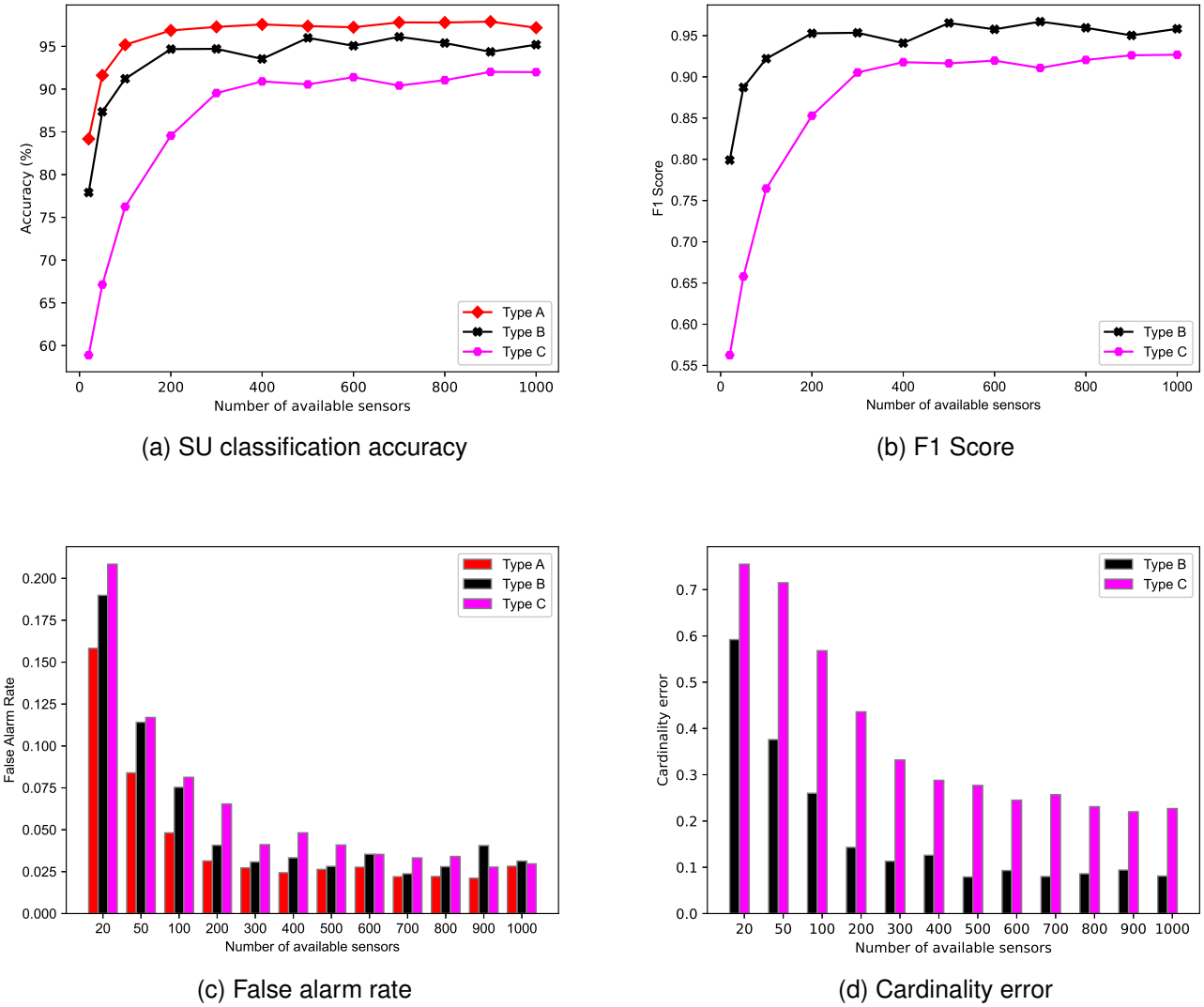
$$\text{Cardinality error} = \frac{C_e}{C_t}, \quad (9)$$

where C_e represents the number of test samples where the model's violator count estimate is incorrect, and C_t is the total number of test samples.

C. Impact of Sensor Availability

We assess Spec-GNN's capability to correctly classify SUs and identify violators under varying sensor quantities available to the spectrum manager. To achieve this, we simulate test scenarios whose configuration involves a specific number of sensors. For each sensor count, outage scenarios were simulated for each of the three outage types with 1,000 test samples generated for each type. The locations of the sensors, along with all other simulation parameters including the number and locations of SUs and violators, were randomized for each sample based on the settings outlined in section V-A. We test the performance for a range of 20 to 1000 sensors available in the 10 km x 10 km area. A maximum amount of 1000 sensors was evaluated due to limitations in our computing memory. As can be observed by the results in Fig. 4, Spec-GNN's performance generally improves across all metrics as the amount of sensors increase. This improvement is because with a higher sensor density, the input graph more suitably represents the spectrum environment due to larger amount of information on the outage provided by the higher number of sensors. We observe this trend across all outage types. For a per type comparison, we observe that irrespective of the number of available sensors, Spec-GNN generally performs best in Type A outage scenarios and the worst in Type C scenarios. For sensor counts above 300, the model is able to achieve accuracy of around 90% for the Type C outage and up to 95% for Type A, with Type B ranging in between. Spec-GNN simultaneously achieves an FAR of at most 0.05, with the FAR even going as low as 0.025 when there are up to 1000 sensors for all outage types. For the same sensor range, Spec-GNN also achieves high F1 scores of above 0.9, and low cardinality error below 0.1 for Type B. Note that we do not evaluate F1 score and cardinality error for Type A outage since there is no presence of violators in that scenario. The precision and recall values used to compute the F1 scores are outlined in Table III and Table IV respectively.

Spec-GNN's performance in which it performs better for Type A and worst for Type C intuitively makes sense. Type A outage scenarios may be seen as the least complex outage type as the outage is caused solely by unexpected environmental noise and there are no SU violators. Hence, Spec-GNN does not have to deal with any uncertainties due to active violators in the system which explains it's good performance even with a low amount of sensors - impressively achieving more than 90% accuracy even with only 50 sensors (0.00005% sensor density). Meanwhile, Type C outage may be regarded as the most complex as its outage is due to a combination of both



(a) SU classification accuracy

(b) F1 Score

(c) False alarm rate

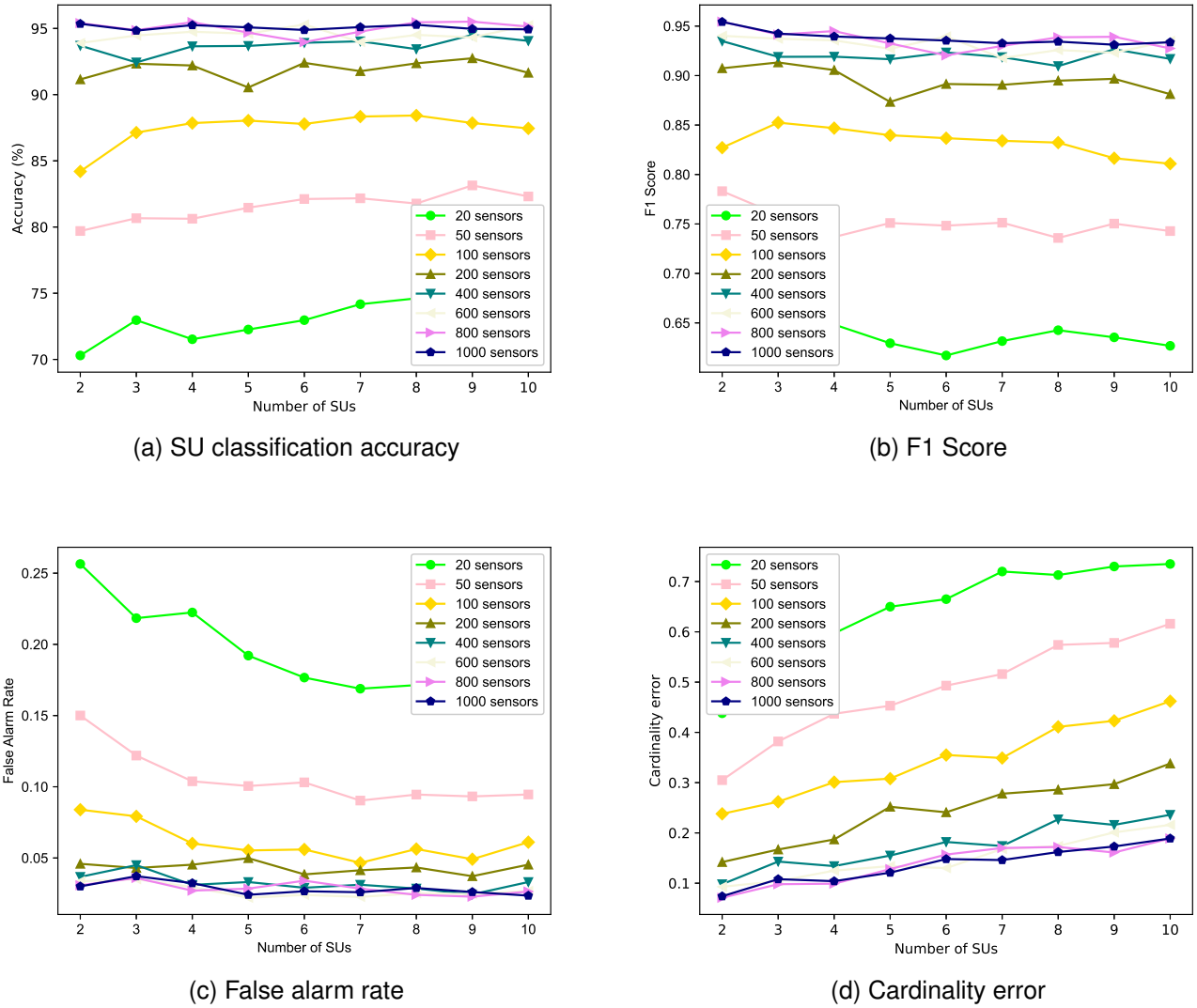
(d) Cardinality error

Fig. 4. Spec-GNN's performance across varying numbers of available sensors during Type A, B, and C outage scenarios. Subfigures (a), (b), (c), and (d) show the classification accuracy, F1 score, false alarm rate, and cardinality error, respectively, as the number of sensors accessible to the spectrum manager varies. We observe that Spec-GNN's performance generally improves across all metrics as the sensor count increases. Additionally, Spec-GNN performs best in Type A outage scenarios and worst in Type C scenarios.

SU violators and unforeseen noise. This explains why Spec-GNN performs worst across all metrics for its scenario. Type B is in between the aforementioned two in complexity, which also reflects in the observed results. Additionally, we observe that Spec-GNN suffers performance degradation due to low amount of sensors most notably for the Type C outage case. At sensor counts below 300, we observe a huge performance gap between Type C and the other outage types. However, as the sensor density increases, there is a notable reduction in the performance gap, which indicates that the Type C violation scenario would benefit most from the availability of good sensor coverage. Overall, the results indicate that Spec-GNN still delivers reasonably good performance in the midst of challenging scenarios such as very low sensor density. When there is access to as few as 200 sensors in the 10 km x 10 km spectrum area (0.0002% sensor density), Spec-GNN is still able to achieve as much as 95% accuracy for the Type A outage and 85% accuracy for the more complex Type C, with under 0.03 and 0.075 FAR respectively for the two types.

D. Impact of the amount of SUs participating in the DSA system

In this evaluation, we assess Spec-GNN's effectiveness in identifying violators under varying amount of SUs for different sensor counts. Each test scenario involved simulating outage for a specific number of SUs and sensor count. 1,000 test samples were generated for each SU-sensor configuration with all other simulation parameters including the outage type randomized per sample. From Fig. 5, we observe that for the different sensor counts, although not so significant, there is a slight decrease in both FAR and F1 score as the number of SUs increase. This indicates that in general, Spec-GNN



(a) SU classification accuracy

(b) F1 Score

(c) False alarm rate

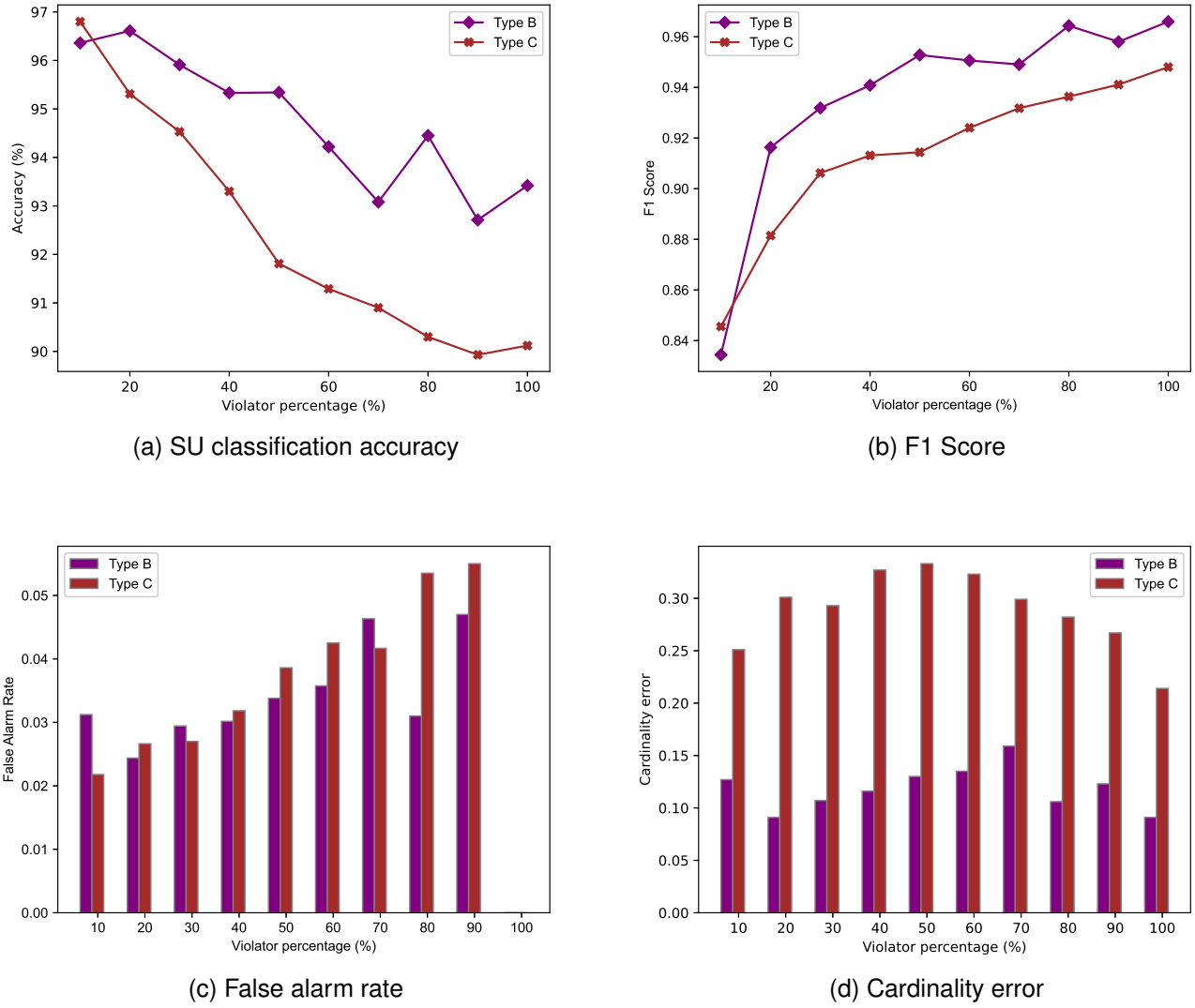
(d) Cardinality error

Fig. 5. Figure depicting Spec-GNN's effectiveness in identifying violators under varying numbers of secondary users and sensor counts. The results indicate that Spec-GNN maintains robust performance even with a large number of DSA participants, particularly when sensor coverage is sufficient.

learns to adapt to the presence of more participating SUs in the DSA system by being slightly more cautious in classifying additional SUs as violators, which also in turn reduces its F1 score. We observe that this adaptation is more significant for the lower sensor counts below 100 sensors. This could be because the dearth of information provided by very low sensor densities prompts the model to learn to be even more cautious under such conditions, which could result in some positive effect on its overall accuracy if its precision and recall are not so much affected. For the higher sensor counts, the F1 score and FAR similarly decrease at very low rates thereby causing changes in the overall accuracy to be minimal. For the cardinality error, we observe in Fig. 5d, that it increases as the number of SUs rise for all sensor counts. We infer this is because as the model's F1 score decreases with an increase of participating SUs, it becomes more difficult for it to determine the exact number of violators at any given time due to higher uncertainty incurred by the larger number of possible culprits. However, this degradation is much less significant for the larger sensor counts as the cardinality error is still under 0.2 even at the maximum number of SUs. In general, we conclude that Spec-GNN is robust to change in the number of SUs participating in the spectrum sharing process, and performs reasonably well even for a high number of DSA participants at any given time. This robustness is especially prominent for scenarios where the spectrum manager has access to information from a fairly good amount of monitoring sensors.

E. Impact of Violator Proportion

We also perform experiments to assess how the proportion of violators affects Spec-GNN's effectiveness. For varying percentages of SUs which are violators, we simulate test scenarios in which the spectrum manager grants spectrum



(a) SU classification accuracy

(b) F1 Score

(c) False alarm rate

(d) Cardinality error

Fig. 6. Spec-GNN's performance in Type B and C outage scenarios as the percentage of violators among secondary users ranges from 10% to 100%. Each test scenario was configured with 10 SUs and 1000 sensors. We observe that Spec-GNN maintains strong performance, even when a high proportion of the active SUs are violators.

access to the maximum number of SUs, and has access to the maximum number of sensors deployed in the spectrum area i.e. 10 and 1000 respectively. Outages were simulated for B and C outage types with 1,000 test samples generated for each type. The identities of the violators are selected randomly among the SUs in each sample. All other simulation parameters including the locations of the sensors and SUs are also randomized using the settings as described in Section V-A. Fig. 6 shows Spec-GNN's performance across accuracy, F1 score, FAR, and cardinality error as the percentage of active violators varies for the different outage types. In Fig. 6a, we observe that the classification accuracy generally drops as the the violator percentage increases for both Type B and C scenarios. However, Type C outage generally has lower accuracy which we as earlier inferred, is due to its more complex violation caused by a combination of violator transmissions and unforeseen noise, which adds greater uncertainty during the model's inference. This is in contrast to that of Type B which is due solely to violator transmission with no unexpected noise. Nonetheless, for both types, Spec-GNN still achieves quite impressive results with accuracy of at least 90% when all the SUs are violators, and close to 92% when the violators make up to half of the total number of SUs. We also observe the impact of the percentage of violators on the F1 score and FAR as shown in Figs. 6b and 6c respectively. We see that both metrics generally increase with a rise in the proportion of violators. We infer this is because as a higher number of SUs contribute to the observed violation, the sum violation power increases which results in Spec-GNN having higher uncertainty in determining which of the SUs are non-violators and as such, it tends towards more easily classifying an SU as a violator. Hence, although its F1 score increases due to higher number of true positives, the probability with which it wrongly classifies innocent SUs as violators increases.

TABLE III
PRECISION SCORES ACROSS A VARYING AMOUNT OF SENSORS.

Outage type	Number of available sensors											
	20	50	100	200	300	400	500	600	700	800	900	1000
Type B	0.85	0.91	0.94	0.97	0.98	0.97	0.98	0.97	0.98	0.98	0.97	0.98
Type C	0.76	0.87	0.92	0.94	0.97	0.96	0.97	0.97	0.97	0.97	0.98	0.98

TABLE IV
RECALL SCORES ACROSS A VARYING AMOUNT OF SENSORS.

Outage type	Number of available sensors											
	20	50	100	200	300	400	500	600	700	800	900	1000
Type B	0.75	0.86	0.9	0.94	0.93	0.91	0.95	0.94	0.95	0.94	0.93	0.94
Type C	0.45	0.53	0.65	0.78	0.85	0.88	0.87	0.87	0.86	0.87	0.88	0.88

TABLE V
PRECISION SCORES ACROSS A VARYING PROPORTION OF VIOLATORS FOR A SETTING OF 10 SUS AND 1000 SENSORS.

Outage type	Violator percentage (%)									
	10	20	30	40	50	60	70	80	90	100
Type B	0.77	0.9	0.93	0.95	0.97	0.97	0.98	0.99	0.99	1.0
Type C	0.82	0.89	0.93	0.95	0.96	0.97	0.98	0.99	0.99	1.0

TABLE VI
RECALL SCORES ACROSS A VARYING PROPORTION OF VIOLATORS FOR A SETTING OF 10 SUS AND 1000 SENSORS.

Outage type	Violator percentage (%)									
	10	20	30	40	50	60	70	80	90	100
Type B	0.92	0.93	0.93	0.93	0.94	0.93	0.92	0.94	0.92	0.93
Type C	0.88	0.87	0.88	0.88	0.87	0.88	0.89	0.89	0.89	0.9

In this case, the FAR increases at a higher rate than the F1 score, which results in a general decrease of accuracy as the violator count increases. Nonetheless, because of good sensor coverage, even in bad scenarios where the violator count is at an equal or greater percentage than non-violators, the model's FAR is still below 0.04 and 0.06 respectively. This indicates that Spec-GNN is robust in the face of extreme scenarios where there may be more dishonest than honest SUs in the DSA system. Tables V and VI delineate the precision and recall scores that constitute the F1 score. We also note that we cannot ascertain a clear relationship between the variation in violator proportion and cardinality error, although it appears that the error seems to be at its highest when the violator percentage ranges from 40% to 60%, somewhat indicating that Spec-GNN has the highest uncertainty in estimating the true violator count when there is an equal number of violators and non-violators. This could indicate that Spec-GNN learns features that are better at determining the true violator count when either the amount of violation in the system is very small or very large.

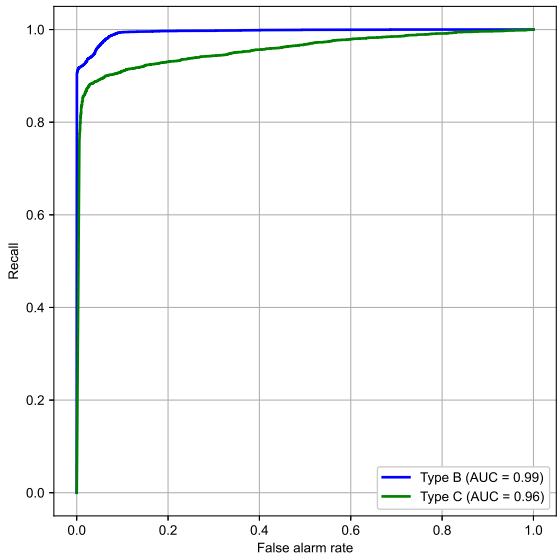


Fig. 7. Receiver operating characteristic (ROC) curve for Spec-GNN in Type B and C outage scenarios.

F. Implication of false alarms and missed detections

In addition to evaluating Spec-GNN's performance, it is important to consider the system-level consequences of classification errors in the spectrum enforcement process. A false alarm involves incorrectly identifying a compliant SU as a violator. In a practical system, this could result in unjust enforcement actions such as spectrum access revocation or financial penalties, potentially undermining SU trust and incurring legal or reputational costs for the spectrum manager. On the other hand, a missed detection occurs when a true violator is not flagged, allowing continued over-transmission

that threatens PU protection and may result in extended outage durations. If repeated, such failures could lead the PU to lose confidence in the enforcement system and ultimately opt out of the sharing framework.

These opposing risks underscore the need for policy-aware enforcement that carefully balances PU protection with the cost of unjust penalties against compliant SUs. To evaluate how Spec-GNN manages this trade-off, Fig. 7 presents the model's receiver operating characteristic (ROC) curve, constructed from test scenarios involving both Type B and Type C outages. For each violation type, 1000 test samples were generated, with the number of participating SUs and violator identities randomly selected per instance. Each sample was evaluated using the maximum number of available sensors to reflect the best-case sensing condition.

The ROC curve illustrates how Spec-GNN's detection sensitivity (recall) varies as a function of the false alarm rate. As discussed earlier, the model performs better in Type B outages compared to the more complex Type C scenario. From Fig. 7, we observe that Spec-GNN can achieve a recall of up to 1 in Type B scenarios while maintaining a false alarm rate around 0.1, and up to 0.9 recall in Type C scenarios under the same threshold. Even under a stricter tolerance of less than 0.01 false alarm rate, Spec-GNN maintains over 0.9 recall in Type B cases. Furthermore, the area under the ROC curve (AUC) exceeds 0.95 for both outage types, indicating consistently high classification performance across varying decision thresholds.

These results demonstrate that Spec-GNN provides a flexible enforcement mechanism that enables spectrum managers to adjust decision thresholds based on their operational priorities, favoring strict PU protection or SU fairness, without significantly compromising accuracy.

VI. Conclusion and future work

In this paper, we addressed the novel problem of identifying spectrum violators in an underlay DSA system. We first defined three types of outages that may arise in such systems, and then we proposed Spec-GNN, a novel GNN based algorithm that pinpoints which spectrum violators, if any, are responsible for an outage. Post outage detection, a spectrum graph constructed from sensor power measurements and SU power limits, serves as input to the Spec-GNN model, which classifies SUs as either violators or non-violators. Spec-GNN was evaluated across diverse outage scenarios, demonstrating robust performance with an SU classification accuracy of around 92% for all outage types even when violators constituted up to 50% of the SUs participating in the DSA system, while maintaining the false alarm rate to be below 0.04. Future research directions include validating Spec-GNN in real-world experiments, and investigating potential adversarial attacks that may impact its effectiveness.

Also, while Spec-GNN focuses on identifying violators following an outage, the specific enforcement response taken by the spectrum manager, such as dynamic power reallocation, SU blacklisting, or real-time revocation of access, depends on the operational and regulatory context and is not addressed in this work. Additionally, although the model outputs violator labels, enhancing the interpretability of these predictions is important for regulatory transparency. Future extensions could incorporate explainable GNN methods to provide insights into the decision logic behind each violator classification, thereby supporting legal or policy-driven enforcement actions.

References

[1] E. Hossain, D. Niyato, and Z. Han, *Dynamic spectrum access and management in cognitive radio networks*. Cambridge university press, 2009.

[2] J. Mitola and G. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[3] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[4] F. Hu, B. Chen, and K. Zhu, "Full spectrum sharing in cognitive radio networks toward 5g: A survey," *IEEE Access*, vol. 6, pp. 15 754–15 776, 2018.

[5] M. G. Khoshkholgh, K. Navaie, and H. Yanikomeroglu, "Access strategies for spectrum sharing in fading environment: Overlay, underlay, and mixed," *IEEE Transactions on Mobile Computing*, vol. 9, no. 12, pp. 1780–1793, 2010.

[6] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[7] T. C. Clancy, "Achievable capacity under the interference temperature model," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, 2007, pp. 794–802.

[8] R. Menon, R. Buehrer, and J. Reed, "Outage probability based comparison of underlay and overlay spectrum sharing techniques," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, 2005, pp. 101–109.

[9] G. I. Tsiropoulos, O. A. Dobre, M. H. Ahmed, and K. E. Baddour, "Radio resource allocation techniques for efficient spectrum access in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 824–847, 2016.

[10] A. Dutta and M. Chiang, ""see something, say something" crowdsourced enforcement of spectrum policies," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 67–80, 2016.

[11] C. Zhan, H. Gupta, A. Bhattacharya, and M. Ghaderibaneh, "Efficient localization of multiple intruders in shared spectrum system," in *2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2020, pp. 205–216.

[12] F. Mitchell, A. Baset, N. Patwari, S. K. Kasera, and A. Bhaskara, "Deep learning-based localization in limited data regimes," in *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning*, ser. WiseML '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 15–20. [Online]. Available: https://doi.org/10.1145/3522783.3529529

[13] C. Zhan, M. Ghaderibaneh, P. Sahu, and H. Gupta, "Deepmtl pro: Deep learning based multiple transmitter localization and power estimation," *Pervasive and Mobile Computing*, vol. 82, p. 101582, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119222000311

[14] C. Ezemaduka and A. A. Abouzeid, "Privacy-aware deep learning based localization of spectrum violators," in *2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, 2023, pp. 98–106.

[15] J. (Jerry) Park, V. Kumar, and T. Oyedare, *Policy Enforcement in Dynamic Spectrum Sharing*, 2019, pp. 341–359.

[16] C. Galiotto, G. K. Papageorgiou, K. Voulgaris, M. M. Butt, N. Marchetti, and C. B. Papadias, "Unlocking the deployment of spectrum sharing with a policy enforcement framework," *IEEE Access*, vol. 6, pp. 11 793–11 803, 2018.

[17] M. A. A. Careem, A. Dutta, and W. Wang, "Spectrum enforcement and localization using autonomous agents with cardinality," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 702–715, 2019.

[18] M. A. A. Careem and A. Dutta, "Sensechain: Blockchain based reputation system for distributed spectrum enforcement," in *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019, pp. 1–10.

[19] D. Das, J. Rose, T. Znati, P. Bustamante, M. Weiss, and M. M. Gomez, "Spectrum misuse detection in cooperative wireless networks," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, 2020, pp. 1–6.
[20] M. Li, D. Yang, J. Lin, M. Li, and J. Tang, "Specwatch: A framework for adversarial spectrum monitoring with unknown statistics," *Computer Networks*, vol. 143, pp. 176–190, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128618305255
[21] L. Zhang, G. Ding, Q. Wu, and Z. Han, "Spectrum sensing under spectrum misuse behaviors: A multi-hypothesis test perspective," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 993–1007, 2018.
[22] V. Kumar, H. Li, J.-M. J. Park, and K. Bian, "Crowd-sourced authentication for enforcement in dynamic spectrum sharing," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 625–636, 2019.
[23] ——, "Enforcement in spectrum sharing: Crowd-sourced blind authentication of co-channel transmitters," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2018, pp. 1–10.
[24] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "Specguard: Spectrum misuse detection in dynamic spectrum access systems," *IEEE Transactions on Mobile Computing*, vol. 17, no. 12, pp. 2925–2938, 2018.
[25] A. Nika, Z. Zhang, B. Y. Zhao, and H. Zheng, "Toward practical spectrum permits," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 1, pp. 112–122, 2017.
[26] X. Zhang, P. Huang, Q. Jia, and L. Guo, "Cream: Unauthorized secondary user detection in fading environments," in *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2018, pp. 406–414.
[27] Q. Pei, B. Yuan, L. Li, and H. Li, "A sensing and etiquette reputation-based trust management for centralized cognitive radio networks," *Neurocomputing*, vol. 101, pp. 129–138, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231212006418
[28] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019.
[29] S. Parsaeefard and A. R. Sharafat, "Robust distributed power control in cognitive radio networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 4, pp. 609–620, 2013.
[30] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Transactions on Wireless Communications*, vol. 6, no. 2, pp. 649–658, 2007.
[31] I. Mitliagkas, N. D. Sidiropoulos, and A. Swami, "Convex approximation-based joint power and admission control for cognitive underlay networks," in *2008 International Wireless Communications and Mobile Computing Conference*, 2008, pp. 28–32.
[32] A. G. Marques, X. Wang, and G. B. Giannakis, "Dynamic resource management for cognitive radios using limited-rate feedback," *IEEE Transactions on Signal Processing*, vol. 57, no. 9, pp. 3651–3666, 2009.
[33] E. Dall'Anese, S.-J. Kim, G. B. Giannakis, and S. Pupolin, "Power control for cognitive radio networks under channel uncertainty," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3541–3551, 2011.
[34] X. Gong, S. A. Vorobyov, and C. Tellambura, "Optimal bandwidth and power allocation for sum ergodic capacity under fading channels in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 4, pp. 1814–1826, 2011.
[35] R. Zhang, "On peak versus average interference power constraints for protecting primary users in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 2112–2120, 2009.
[36] C. Jiang, Y. Chen, K. R. Liu, and Y. Ren, "Renewal-theoretical dynamic spectrum access in cognitive radio network with unknown primary behavior," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 3, pp. 406–416, 2013.
[37] S. Stotas and A. Nallanathan, "On the throughput and spectrum sensing enhancement of opportunistic spectrum access cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 97–107, 2012.
[38] M. Khaledi, M. Khaledi, S. Sarkar, S. Kasera, N. Patwari, K. Derr, and S. Ramirez, "Simultaneous power-based localization of transmitters for crowdsourced spectrum monitoring," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 235–247. [Online]. Available: https://doi.org/10.1145/3117811.3117845
[39] A. Chakraborty, M. S. Rahman, H. Gupta, and S. R. Das, "Specsense: Crowdsensing for efficient querying of spectrum occupancy," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017, pp. 1–9.
[40] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2021.
[41] W. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in *Advances in Neural Information Processing Systems*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds., vol. 30. Curran Associates, Inc., 2017.
[42] M. Gupta and S. Prakriya, "Performance of multiuser uplink underlay noma networks with channel knowledge," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 4, pp. 6000–6005, 2024.
[43] ——, "Performance of csi-based power control and noma/oma switching for uplink underlay networks with imperfect sic," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1753–1769, 2022.
[44] M. Bocca, O. Kaltiokallio, N. Patwari, and S. Venkatasubramanian, "Multiple target tracking with rf sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1787–1800, 2014.

Chibuikem Ezemaduka received the B.Eng. degree in communication engineering from the Department of Electrical and Electronic Engineering at the Federal University of Technology, Owerri, Nigeria, in 2018, and the M.S. degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, in 2024. He is currently pursuing the Ph.D. degree with the Department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute. His current research interests include wireless communications, computer networking, and machine learning.

Alhussein Abouzeid (Senior Member, IEEE) received the B.S. degree with honors from Cairo University, Egypt, in 1993, and the M.S. and Ph.D. degrees from the University of Washington, Seattle, in 1999 and 2001, respectively, all in electrical engineering. He is currently a Professor with the Department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute, Troy, NY. He has served as a program director with the U.S. National Science Foundation (NSF) from 2008 to 2010 and 2022 to 2025, where he co-founded several advanced networking research funding programs such as EARS, RINGS and VINES. He held appointments with University of Oulu in Finland, Allied Signal (now Honeywell), Hughes Research Labs (HRL), and Alcatel Telecom. His research interests include computer networking with an emphasis on wireless systems. His research has been supported by NSF and the National Institutes of Health (NIH). Dr. Abouzeid has served as Associate Editor for the IEEE Transactions on Wireless Communications and the IEEE Transactions on Mobile Computing. He is a recipient of the NSF CAREER Award, the Finnish FiDiPro Fellowship, and several best paper awards.