On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks

Anastasia Tsiota, Dionysis Xenakis, Nikos Passas, and Lazaros Merakos

***Abstract*—The proliferation of radio-enabled equipment, including sensors, controllers, actuators, mobile handhelds, etc., into the today's heterogeneous wireless network (HWN) has led to the support of different vertical services on-top of the same physical infrastructure. Such an approach increases the potential for enhanced multiplexing gains due to the joint utilization of multiple network tiers and their resources. However, it also links the availability of new services to the robustness of the HWN infrastructure against malicious attacks. In this paper, we study the impact of two prominent denial of service (DoS) attacks, the jamming and the black hole attack, on network coverage of multi-tier HWNs. In particular, we consider a HWN model of multiple tiers, where the locations of nodes belonging to each tier are modeled by a homogeneous Poisson point process (PPP) with known intensity. Each tier consists of regular nodes, jammers (disrupting downlink communications by transmitting at constant power), and black holes (appearing as regular nodes but without forwarding received packets to their legitimate destination). The type of a node for a given network tier is determined by a prescribed probability, whereas jammer and black hole nodes are considered to act independently from each other. We further focus on the challenging scenario where end users can access a limited number of network tiers, while we also allow different tiers to potentially utilize different spectrum bands. Assuming that successful service reception from a node belonging to a given network tier requires a minimum received signal quality threshold to be attained, we derive exact expressions and performance bounds on the coverage probability of random multi-tier HWNs with joint jamming and black hole attacks, which depend on the capability of network nodes to detect and avoid association with malicious nodes (i.e., jammers or black holes). Detailed numerical results highlight the usefulness of the proposed analysis, providing valuable insights on system design and parameterization towards enhanced network robustness.**

***Index Terms*—Heterogeneous wireless networks, multi-tier networks, jamming, black hole attacks, performance analysis.**

I. Introduction

Our community has recently witnessed an explosive increase in the number and diversity of end devices with wireless communication capabilities. Mobile phones, smart meters, wearables, connected vehicles and drones, are only a few examples in the area. Recent reports predict that the number of mobile phones will reach a total of 8.6 billion devices by 2022, while wide-area and short-range Internet of Things (IoT) devices are expected to surpass the number of mobile phones by 2022 [1]. This trend has created a highly dynamic and multi-tier heterogeneous wireless network (HWN), which is composed of wireless networking elements (WNEs) of different-purpose, supporting different radio access technologies (RATs). Adding to this, the forthcoming integration of different vertical services and RATs under the 5G mobile network architecture, using potentially the same physical resources, stresses the need for a holistic analysis on device coexistence in both licensed and unlicensed spectrum. Besides, 3GPP has already specified how LTE can expand its operation to unlicensed bands with incumbent IEEE networks (e.g., License Assisted Access at 5GHz in Release 13). Similar capabilities are provisioned for the 3GPP New Radio as well.

Support of different vertical services and RATs on top of the same physical resources, inevitably links service availability to network robustness against malicious attacks. *Denial of Service* (DoS) attacks have lately increased both in numbers and sophistication [3]. DoS attacks are performed by malicious nodes that aim to make a machine, or network resource, unavailable to legitimate users. DoS attacks, and distributed DoS in particular, have attracted surge of interest due to the severe impact that they can potentially have on our everyday life activities and working routine [4]. One recent DoS attack with disruptive influence on the Danish Railway Company DSB has been recorded in May 2018. The attack made it impossible for travelers to purchase a ticket via the DSB mobile app, website, ticket machines and local kiosks at the stations. DoS attacks have also been reported in October 2017, where several IT systems used by Sweden's transport agencies have been brought down on two separate days.

Wireless networks are more vulnerable to DoS attacks due to the openness of the wireless medium. Wireless DoS (WDoS) attacks aim to prevent legitimate data from reaching their destinations. WDoS attacks can be launched in various layers of a wireless network, including the physical and the network layer. *Jamming attacks* are a special case of WDoS that affect the physical layer. Jamming attacks are performed by an entity widely known as jammer, which aims to disrupt wireless reception of downlink (DL) data by creating interference during the transmission, or reception of packets. The most common form of jamming attacks involves an attacker that emits a strong wireless signal continuously to degrade network coverage. On the contrary, *black hole* attacks typically affect the network layer, as they utilize a set of network nodes that are reprogrammed (by someone malicious) to block (or reject) the packets they receive (or produce) rather than forward them to their destination. Therefore, any information entering the

This Research is supported by the Onassis Foundation under the "Special Grant & Support Program for Scholars' Association Members" (Grant No. R ZN 003/2017-2018).

A. Tsiota, D. Xenakis, N. Passas and L. Merakos are with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Greece. Email: {atsiota, nio, passas, merakos}@di.uoa.gr.

coverage area of black hole nodes is discarded, or processed to extract sensitive information. Black hole attacks are easy to deploy and can compartmentalize the network by undermining the effectiveness of two-way end-to-end information flow.

In this paper, we study the performance of multi-tier HWNs that are under the joint impact of jamming and black hole attacks. We model the locations of network nodes using a tractable multi-tier model of Poisson point processes (PPPs), which enables us to estimate network coverage in closed-form. In particular, we derive network coverage for two scenarios of high practical interest. In the first scenario, termed as the *perfect detection of malicious WNEs* scenario, we derive network coverage assuming that end users can perfectly detect jammer and black hole WNEs and avoid association with them. To achieve this, we first derive network coverage for accessible tiers belonging to a given frequency band b (Theorem 1) and extend the respective result to the scenario where multiple bands can be assessed by the end users (Corollary 1). The expressions derived in this scenario provide an upper performance bound on network coverage of random multi-tier HWNs with joint jamming and black hole attacks, as they assess network coverage for any countermeasure that can achieve perfect detection (and avoidance) of malicious WNEs.

In the second scenario, termed as the *no detection of malicious WNEs* scenario, we derive network coverage assuming that end users are fully unable to detect malicious nodes, allowing thus association with WNEs independent of their type (regular, or not). In this scenario, network coverage strongly depends on the association policy followed by end users, i.e., how they prioritize access across reachable WNEs that belong to different network tiers, operate in different spectrum bands, or utilize different radio access technologies (RATs). To this end, for this scenario, we assess network coverage under general association policies that prioritize access across WNEs based on the operating spectrum band (Theorem 2). To achieve this, we build on the results derived for the *perfect detection of malicious WNEs* scenario and derive the association probability with a WNE operating in a given frequency band independent of its type (Corollary 2). The optimal policy for band prioritization (i.e., the one maximizing the coverage probability) is also discussed for this scenario (Proposition 1). Detailed numerical results draw useful design guidelines for practical HWN deployments, also providing valuable insights on upper and lower performance bounds for network coverage in HWNs with jamming and black hole attacks.

II. Related Works and Main Contributions

Current literature includes numerous studies that either aim to assess the impact of jamming/black hole attacks on network performance, or aim to develop efficient countermeasures to safeguard the performance of different network types from such attacks. The vast majority of recent studies in the area focus on Wireless Sensor Networks (WSNs) [5] - [10]. In [5], a novel routing scheme is proposed to dynamically avoid black hole areas, by estimating the behavioral patterns and the locations of black hole nodes. To avoid DoS and compromised node attacks in WSNs, the authors in [6] consider random multi-path routing. Four different algorithms are proposed to split the original message into segments and randomly route the segments through multiple network paths. Network robustness is assessed in terms of the packet interception probability (ratio of intercepted packets to the number of source packets). The impact of different types of system failure on the WSN performance is quantified in [7]. Based on continuous time markov chain (CTMC) modeling, network performance is analyzed in terms of network survivability under node, link and attack failures. The impact of multichannel jamming attacks under mission-critical applications is investigated in [8], where the authors consider a WSN dedicated to the tracking of moving targets, such as airplanes and military warcrafts. The authors in [9] overview different types of jamming and eavesdropping attacks in industrial WSNs, review relevant countermeasures and highlight four main reasons that degrade system reliability: interference, path loss, multipath fading and link failure. Assuming a small sample of network elements (source, destination, jammer, eavesdropper, relay), a simulation-driven performance comparison of different schemes is provided, using quality of service (QoS) metrics. The authors in [10] focus on wireless network-controlled systems (WNCS) of physical elements (plants, sensors, controllers and actuators) that communicate through wireless networks. Assuming that the performance of the WNCS is described by a linear quadratic Gaussian control cost function, the authors derive an optimal strategy to maximize the impact of jamming attacks in WNCS given specific energy and system stability constraints.

The works in [11] and [12] focus on mobile ad hoc networks (MANETs). The problem of black hole attacks in MANETs is reviewed in [11], where a modification of the on-demand routing protocol is proposed to alleviate black hole attacks. A suite of protocols to secure MANETs against different types of malicious attacks is proposed in [12], and their performance is analytically assessed. The impact of jamming attacks in cognitive radio networks (CRNs) with energy harvesting is studied in [13], assuming that secondary users perform deception transmissions to deplete the battery of jammer nodes. An optimal strategy to maximize end-to-end throughput is also derived, using Markov decision modeling and machine learning. The impact of jamming against wireless networks composed of base stations, or access points (APs), is studied in [14]. The locations of legitimate and jammer nodes are modeled using Poisson and Binomial Point Processes, respectively, and closed-form expressions are derived for network outage and error probability in such networks. A meticulous study on friendly jamming is provided in [15], where low-functionality APs cannot detect unauthorized transmissions. To overcome this limitation, external devices (termed as friendly jammers) are used to protect the APs by jamming unauthorized signals. Real-life implementation and simulation results are provided for an IEEE 802.11 campus network.

Different from the studies in [5] - [13], this work studies the performance of multi-tier HWNs that are under the joint impact of constant jamming (fixed transmit power) and black hole attacks, where the locations of jammer and black hole nodes are distributed at random in the Euclidean space with a given probability. On the other hand, different from the studies in [14] and [15], in this work we model the locations of network nodes using a tractable multi-tier model of independent PPPs that enables us to derive upper and lower performance bounds for network coverage, depending on the capability of network nodes to perfectly detect (or not) malicious nodes. Detailed numerical results allows us to draw useful design guidelines for practical network deployments and assess the performance gains of different system design approaches. The main contributions of our work can be summarized as follows:

- We develop a tractable framework to analyze the network coverage performance of multi-tier HWNs in the presence of constant jamming and black hole attacks.
- We derive upper and lower performance bounds on network coverage of multi-tier HWNs with jamming and black hole attacks, depending on the capability of network nodes to perfectly detect (and avoid) malicious nodes.
- We propose and validate the performance of an optimal association strategy that alleviates such attacks when legitimate nodes are unable to detect malicious WNEs.
- We assess the impact of key parameters related to jamming and black hole attacks (e.g. transmit power, attack probability, density of attackers) on network coverage.
- We quantify the performance gains of utilizing multiple spectrum bands, or RAT interfaces, and assess the performance of different frequency-based association strategies.
- We draw guidelines on how to exploit the presented expressions, the derived performance bounds and the proposed countermeasures in practical HWN deployments.

The remainder of this paper is organized as follows. In section III, we present the proposed M-tier HWN system model, define our performance metrics and discuss issues relevant to the use of the proposed mathematical models. In section IV, we derive closed-form expressions on network coverage of multi-tier HWNs with joint jamming and black hole attacks, under two different scenarios of high practical interest. In the first scenario, we assume that legitimate nodes can perfectly detect and avoid association with malicious WNEs (upper performance bound - section IV.A), whereas in the second scenario we assume that legitimate nodes are unable to detect malicious WNEs (lower performance bound - section IV.B). For the second scenario, we further propose an optimal association strategy that enables legitimate nodes to prioritize access among accessible network tiers to maximize network coverage. In section V, we provide detailed numerical results using the presented mathematical analysis in practical HWN deployments and evaluate the efficiency of employing different countermeasures, or system design options. In section VI, we overview our contributions and conclude this work.

III. System Model

A. System Description

We consider a HWN infrastructure of M network tiers, where each tier consists of WNEs that serve similar communication purposes and support the same RAT. WNEs belonging to the m-th tier are termed as tier-m WNEs and their locations are assumed to be distributed according to a homogeneous PPP Φ_m of intensity λ_m in the Euclidean plane with $m \in \mathbb{M} = \{1, \cdots, M\}$. The locations of WNEs belonging to different tiers are assumed mutually independent (i.e., the processes Φ_m are mutually independent). WNEs belonging to different tiers can operate in different spectrum bands, utilize diverse transmit powers, or be characterized by different spatial densities. Nevertheless, WNEs of the same tier are considered to operate in the same spectrum band and utilize the same (fixed) transmit power (if not malicious). In the sequel, we denote by P_m the transmit power of all *regular* (i.e., non-malicious) WNEs belonging to tier-m.

Without loss of generality, we focus on the performance of DL communications of a tagged WNE, termed as the *typical WNE*, which we consider not to be part of the HWN infrastructure (not part of Φ_m, $m \in \mathbb{M}$). The entire HWN is considered to utilize a total of B distinct and non-overlapping spectrum bands, where $B \leq M$ (i.e., different tiers are allowed to utilize the same band). We also denote by $\mathbb{B} = \{1, \cdots, B\}$ the set of utilized spectrum bands and by $\mathbb{M}_b \subseteq \mathbb{M}$ the set of networking tiers that operate in a given band $b \in \mathbb{B}$. Since each tier operates in a single spectrum band, the sets $\mathbb{M}_b$ are disjoint. Radio transmissions in a given spectrum band $b \in \mathbb{B}$ are governed by the same path loss exponent a_b.

We further focus in the challenging scenario where the typical WNE is capable of receiving DL data through multiple tiers of the HWN, e.g. using different RAT interfaces, or antennas. We use $\mathbb{T} \subseteq \mathbb{M}$ to denote the set of *accessible* network tiers. Also, we group the tiers in $\mathbb{T}$ into B disjoint sets (based on their operating band), using $\mathbb{T}_b \subseteq \mathbb{M}_b$ to denote the set of accessible tiers operating in band $b \in \mathbb{B}$. Accordingly, $\mathbb{T} = \cup_{b \in \mathbb{B}} \mathbb{T}_b$. We also consider that successful DL service at the typical WNE requires a minimum received signal quality (RSQ) threshold. For a given accessible tier $\tau \in \mathbb{T}$, we denote this threshold by γ_τ. For analytical tractability, we assume that the RSQ thresholds of all tiers are higher than one (i.e. $\gamma_\tau > 1, \tau \in \mathbb{T}$) and focus our analysis on interference-limited HWNs, where successful data reception is limited by the interference caused by WNEs operating in the same band (i.e. thermal noise at the receiver is assumed to be negligible).

The RSQ threshold assumption implies that the minimum SIR for preserving a successful serving link should be higher than one, or equivalently that the successful reception of data requires a received power from the serving WNE (as measured at the typical WNE) higher than the aggregate interference from all in-band operating and non-serving WNEs. This assumption is typical in works conducting performance analysis using Stochastic Geometry [16] while this assumption has been shown to provide tight upper bounds to the exact solution that relaxes the RSQ threshold higher than one requirement.

B. Jamming and Black Hole Attack Models

Jammer and black hole nodes are considered to act independently with each other, not being in position to deploy collaborative attacks. In more detail, in the sequel we assume that the WNEs of a given tier $m \in \mathbb{M}$ act as jammer or black hole nodes independently from the remainder WNEs in the system, with probability p_m and q_m, respectively, where

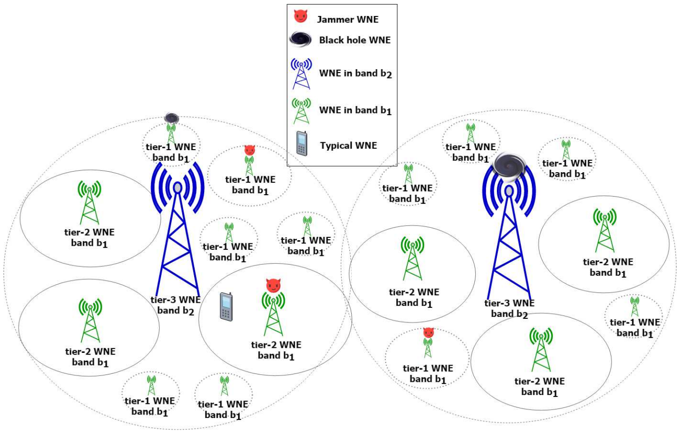


Fig. 1. Example of a three-tier network, where tier-1 and tier-2 WNEs co-utilize band b_1 (blue WNEs) while tier-3 WNEs operate in band b_2.

$0 \leq p_m + q_m \leq 1$. We also consider that all the tier-m jammer WNEs use fixed transmit power, which we denote by J_m. On the contrary, black hole WNEs are considered to act as regular WNEs supporting all necessary signaling procedures (including user association); however, without forwarding received packets to their eligible destinations. To avoid detection of their malicious behavior, black hole WNEs in tier-m are assumed to use the same transmit power P_m with regular WNEs. The analysis followed can be readily extended to the scenario where black hole WNEs use different transmit power compared to regular WNEs.

Since tier-m WNEs act maliciously at random and independently of each other, the point process Φ_m can be further divided into three disjoint and mutually independent PPPs of different intensities. In more detail, the locations of tier-m jammer WNEs can be described by the PPP Φ_{mj} of intensity $p_m \cdot \lambda_m$, the locations of tier-m black hole WNEs by the PPP Φ_{mb} of intensity $q_m \cdot \lambda_m$, and the locations of regular tier-m WNEs by the PPP Φ_{mr} of intensity $(1 - p_m - q_m) \cdot \lambda_m$, where $\Phi_m = \Phi_{mj} \cup \Phi_{mb} \cup \Phi_{mr}$. Notably, this modeling approach is equivalent with a system model where jammer and black hole WNEs are *external* WNEs (not part of the HWN infrastructure) that are distributed at random in the Euclidean plane according to mutually independent PPPs. In Fig.1 we provide an illustrative example of the proposed system model, highlighting the different types of WNEs that are met across the HWN (regular, jammer, black holes) and the potential co-utilization of the same frequency band by different network tiers (i.e., tier-1 and tier-2 WNEs co-utilize band b_1).

C. Performance Metrics

The performance at the typical WNE is assessed in terms of *coverage probability*, taking into account the joint presence of jammer and black hole nodes in the proposed multi-tier HWN model. Aiming to derive upper performance bounds for the coverage probability in such networks, *we do not limit our analysis to a specific association policy* that clearly defines how the typical WNE prioritizes access across the different WNEs. Instead, we consider that the typical WNE is in coverage if there exists at least one WNE $x \in \cup_{m\in\mathbb{M}}\Phi_m$ that satisfies the following properties: i) x is a regular WNE and belongs to one of the accessible tiers in $\mathbb{T}$, i.e., $x \in \cup_{\tau\in\mathbb{T}}\Phi_{\tau r}$, and ii) the Signal to Interference Ratio (SIR) for the WNE x is higher than the RSQ threshold specified for its tier. By letting $SIR(x)$ denote the DL SIR on service reception from WNE x, we formally define the *coverage probability* as follows:

$$\mathcal{C} = P\left[\cup_{\tau\in\mathbb{T}, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right]. \tag{1}$$

Since the proposed M-tier HWN model allows the WNEs to operate in different spectrum bands, the calculation of the coverage probability at the typical WNE strongly depends on the number of spectrum bands available in the system as well as the density and transmission profile of occupants operating in the accessible tiers of $\mathbb{T}$ (Eq. (1)). In the sequel, we consider that the fading power between the typical WNE and a given WNE $x \in \cup_{m\in\mathbb{M}}\Phi_m$ is denoted by h_x and is subject to Rayleigh fading, i.e., the random variables (RVs) h_x are independent and identically distributed with (unitary) exponential distribution. For convenience, we denote by P_x the transmit power of a given WNE $x \in \cup_{m\in\mathbb{M}}\Phi_m$ and by $\|x\|$ its physical distance from the typical WNE. Accordingly, for a given WNE x that operates in band b and belongs to an accessible tier in $\mathbb{T}$, we define the DL SIR $SIR(x)$:

$$SIR(x) = \frac{P_x h_x \|x\|^{-a_b}}{\sum_{m\in\mathbb{M}_b}\sum_{y\in\Phi_m\setminus x} P_y h_y \|y\|^{-a_b}}. \tag{2}$$

Note that the denominator of (2) can be further analyzed based on the transmit power of the different types of WNEs. Accordingly, the total interference experienced in band b at the tagged WNE x, which we denote by $I(x)$, is given by:

$$I(x) = \sum_{m\in\mathbb{M}_b}\Big(\sum_{z\in\Phi_{mj}} J_m h_z \|z\|^{-a_b} + \sum_{y\in\Phi_m\setminus\{x,\Phi_{mj}\}} P_m h_y \|y\|^{-a_b}\Big). \tag{3}$$

Lemma 1 presents a property that is useful in our analysis.

Lemma 1. *In every band $b \in \mathbb{B}$, there can be up to one WNE $x \in \cup_{m\in\mathbb{M}_b}\Phi_{mr}$ to exhibit $SIR(x)$ higher than one.*

Proof. Follows from the assumption of RSQ thresholds per tier higher than one. A similar property has been proved in [16] and for that reason we omit the proof in this paper. □

D. Discussion on the System Model and Parameters

The proposed multi-tier model of randomly and independently distributed heterogeneous WNEs extends the K-tier model for cellular networks presented in [16]. However, different from [16], our model allows the utilization of different spectrum bands across network tiers and enables explicit modeling of the jammer/black hole locations, either as part of the HWN infrastructure, or as an external group of WNEs. Also, the applicability of the proposed M-tier model is not limited to the scenario where the typical WNE associates with the (single) WNE exhibiting the highest SIR [16], but applies to the scenario where multiple WNEs (operating in different bands) meet the RSQ threshold. We now provide an example on how to setup the system model in practical scenarios.

We consider a four-tier HWN infrastructure tailored to the exchange of measurement and control messages in the Smart

Grid. Tier-1 WNEs are low-power sensors receiving DL data from tier-2 smart meters (SMs) through ZigBee in band b_1. Tier-2 WNEs are SMs receiving DL data either from other tier-2 SMs using Wi-Fi based machine-type communications (MTC) in band b_1 (ZigBee/Wi-Fi coexistence), or from tier-3 local data aggregators (LDAs) using Wi-Fi in band b_2. Tier-3 WNEs are LDAs receiving DL data from tier-4 cellular base stations in band b_3. Let the *typical WNE* be an external SM which, in addition to receiving DL data from other tier-2 SMs in band b_1 and tier-3 LDAs in band b_2, it can receive DL data (from the utility operator) through its cellular interface in band b_3. Accordingly, the system model parameters for the typical WNE (the SM) are given as follows: $B = 3$, $\mathbb{B} = \{b_1, b_2, b_3\}$, $M = 4$, $\mathbb{M} = \{1, 2, 3, 4\}$, $\mathbb{M}_1 = \{1, 2\}$, $\mathbb{M}_2 = \{3\}$, $\mathbb{M}_3 = \{4\}$, $\mathbb{T} = \{2, 3, 4\}$, $\mathbb{T}_1 = \{2\}$, $\mathbb{T}_2 = \{3\}$, $\mathbb{T}_3 = \{4\}$.

At this point, it is important to note that the proposed multi-tier HWN model with random jammer and black hole node locations can not be explicitly used to model the evolution of jamming and black hole attacks in the time domain and thus, the impact of specific attack techniques that alter the patterns of jamming in the short term are not explicitly modeled in this work (e.g. random jamming, sweep jamming, reactive jamming). Instead, the present analysis primarily targets to assess the coverage probability of multi-tier networks with randomly-distributed nodes, averaged over all possible network layout instances that pertain a given set of system model characteristics (e.g. network density per tier, transmit power per tier and per node type, probability of having a jamming or black hole attack in a given tier).

As a result, in its current form, the proposed analysis can be viewed as an analytical framework for long-term coverage analysis assuming that jammers employ constant jamming in a given frequency band, or as a framework for single timeslot performance analysis of any type of attack that takes averages over all possible network layouts, assuming that regular, jammer and black hole nodes pertain the system model parameter values defined in section III. Nonetheless, with appropriate matching of the system model parameter values to the characteristics of a given technique, the presented analysis can potentially capture the time aspect of more sophisticated attacks by future works by taking into consideration that a given attack technique will alter the *set of active attackers* in the spatial domain on a per timeslot basis. Such type of performance analysis can be technique-specific and potentially extend the present analytical framework to incorporate the time aspect of different types of jamming and black hole attacks.

IV. Performance Analysis

In this section, we derive exact expressions on the coverage probability of multi-tier HWNs with joint jamming and black hole attacks. We further consider the case where the typical WNE can receive DL data through multiple network tiers (not necessarily simultaneously) and specialize the analysis in two different scenarios of high practical interest. In Section IV.A, we analyze the scenario where the typical WNE can perfectly detect malicious WNEs and avoid association with them, whereas in section IV.B, we analyze the scenario where the typical WNE is fully unable to detect malicious nodes, allowing thus association with WNEs independent of their type (regular, or not). Since different intensities of malicious and regular WNEs are met across the different network tiers, in the second scenario, the coverage probability is shaped by the association policy followed by the typical WNE to prioritize access across the WNEs satisfying the RSQ threshold. Accordingly, in this scenario, we assess the network coverage performance under general association policies that prioritize access across the available WNEs based on the operating spectrum band (or RAT). The optimal policy for band prioritization (i.e. the one maximizing the coverage probability) is also discussed for this particular scenario.

A. Coverage probability: Perfect detection of malicious WNEs

We now consider that the typical WNE can perfectly detect malicious WNEs. Accordingly, the typical WNE is considered to be in coverage if there exists at least one regular WNE that i) belongs to the set of accessible tiers in $\mathbb{T}$ and ii) exhibits a SIR higher than the minimum required RSQ threshold for its tier. We now derive the coverage probability, when the typical WNE can associate only with tiers operating in a particular spectrum band $b \in \mathbb{B}$. We use the term *coverage probability in band* b and the notation $\mathcal{C}_b$ to denote this probability.

Theorem 1. *Assuming that i) the typical WNE can perfectly detect and avoid association with malicious WNEs, and ii) the RSQ threshold for all tiers in* $\mathbb{T}_b$ *is higher than one (i.e.* $\gamma_\tau > 1$ *for all* $\tau \in \mathbb{T}_b$*), the coverage probability* $\mathcal{C}_b$ *is given by:*

$$\mathcal{C}_b = sinc\left(\frac{2\pi}{a_b}\right) \cdot \frac{\sum_{\tau \in \mathbb{T}_b} \lambda_\tau \gamma_\tau^{-\frac{2}{a_b}} (1 - q_\tau - p_\tau) P_\tau^{\frac{2}{a_b}}}{\sum_{m \in \mathbb{M}_b} \lambda_m \left((1 - p_m) P_m^{\frac{2}{a_b}} + p_m J_m^{\frac{2}{a_b}}\right)}. \quad (4)$$

Proof. See Appendix A. □

Note that the coverage probability when the typical WNE can associate with a single tier $\tau \in \mathbb{T}$ can be readily derived by Theorem 1 for $\mathbb{T}_b = \tau$. We omit the result for brevity. Let us now turn our attention to the general scenario where the typical WNE can receive DL data from all accessible tiers in $\mathbb{T}$. In this scenario, there can exist more than one (and up to B) regular WNEs that satisfy the RSQ threshold requirement across the accessible tiers. Corollary 1 extends Theorem 1 to the challenging scenario where the list of accessible tiers in $\mathbb{T}$ utilize multiple spectrum bands (instead of only one as considered in Theorem 1).

Corollary 1. *The coverage probability* $\mathcal{C}$ *in a multi-tier HWN where i) the typical WNE can detect and avoid association with malicious WNEs, ii) the RSQ thresholds for all tiers in* $\mathbb{T}$ *are higher than one, and iii) the tier-*m *WNEs act independently as jammers and black holes with probability* p_m *and* q_m *(*$m \in \mathbb{M}$*), respectively, is given by*

$$\mathcal{C} = 1 - \Pi_{b \in \mathbb{B}} \left(1 - \mathcal{C}_b\right) \quad (5)$$

where $\mathcal{C}_b$ *is derived by Eq. (4).*

Proof. See Appendix B. □

The expressions in Corollary 1 provide an upper performance bound of the coverage probability in multi-tier HWNs that utilize different spectrum bands per tier and are subject to jamming and black hole attacks. Note that the derived expressions can also be used to assess network coverage in multi-tier HWNs that are free of jamming and black hole attacks (i.e. by setting $q_m = 0$ and $p_m = 0$ for all $m \in \mathbb{M}$).

B. Coverage probability: No detection of malicious WNEs

In this section, we consider that the typical WNE is unable to detect malicious WNEs and associates with WNEs independent of their type (i.e. malicious or not). Thus, different from section IV.A, outage events in this scenario also occur due to the association with malicious WNEs. Since the typical WNE cannot distinguish between regular and malicious WNEs, the employment of different association policies result in different coverage probabilities. In the remainder of this section, we consider that the typical WNE prioritizes access among WNEs based on their operating spectrum band. In more detail, we assume that the typical WNE associates with the WNE that satisfies the RSQ requirement for its tier (can be up to one per band - Lemma 1) and operates in the band with the highest possible priority. This association policy is widely used by the today's multi-mode terminals and can be readily generalized to the prioritization of tiers based on their RAT [18].

Without loss of generality, we assume that spectrum bands with lower identifiers are given higher priority, i.e. the typical WNE prioritizes access across bands according to the policy $(\mathbb{T}_1, \cdots, \mathbb{T}_B)$. Provided that up to one WNE can satisfy the RSQ threshold per band (Lemma 1), this policy leads the typical WNE to associate with the WNE that i) belongs to one of the accessible tiers in $\mathbb{T}$, ii) satisfies the RSQ threshold for its tier and iii) operates in the spectrum band with the highest possible priority. Practically, this policy implies that the typical WNE will first search for a WNE that belongs to one of the tiers in $\mathbb{T}_1$ and satisfies the RSQ threshold for its tier. If such a WNE exists, the typical WNE will associate with it without taking into account whether it is of regular, or malicious type (no detection capabilities). In the contrary, if such a WNE does not exists in $\mathbb{T}_1$, the typical WNE will search for a WNE that operates in one of the tiers in $\mathbb{T}_2$ and satisfies the RSQ threshold for its tier, and so on.

In the sequel, for a given band $b \in \mathbb{B}$, we define the association probability as the probability that the typical WNE associates with a WNE (regular or not) in band b. We denote this probability by $\mathcal{A}_b$ and formally define it as follows:

$$\mathcal{A}_b = P\left[\cup_{\tau \in \mathbb{T}_b, x \in \Phi_\tau} \mathbf{1}(SIR(x) > \gamma_\tau)\right]. \tag{6}$$

Note that $\mathcal{A}_b$ corresponds to the probability that at least one WNE (*regular or not*) belonging to an accessible tier in $\mathbb{T}_b$, satisfies the RSQ threshold for its tier. On the other hand, the coverage probability $\mathcal{C}_b$ in (9) corresponds to the probability that at least one *regular* WNE holds the same properties. Thus, by definition, when the typical WNE can detect and avoid association with malicious WNEs, the probabilities $\mathcal{A}_b$ and $\mathcal{C}_b$ are equal. In contrast, when the typical WNE is unable to detect malicious WNEs, the values of $\mathcal{A}_b$ and $\mathcal{C}_b$ are different and depend on the association policy followed by the WNE.

Corollary 2. *Assuming that the typical WNE is unable to detect malicious WNEs and the RSQ thresholds for all tiers in $\mathbb{T}_b$ are higher than one ($\gamma_\tau > 1$, $\tau \in \mathbb{T}_b$), the probability $\mathcal{A}_b$ with which the typical WNE associates with a WNE that operates in band $b \in \mathbb{B}$, belongs to the set of accessible tiers in $\mathbb{T}_b$ and satisfies the RSQ threshold of its tier, is given by:*

$$\mathcal{A}_b = \mathit{sinc}\left(\frac{2\pi}{a_b}\right) \cdot \frac{\sum_{\tau \in \mathbb{T}_b} \lambda_\tau \gamma_\tau^{-\frac{2}{a_b}} \left((1-p_\tau) P_\tau^{\frac{2}{a_b}} + p_\tau J_\tau^{\frac{2}{a_b}}\right)}{\sum_{m \in \mathbb{M}_b} \lambda_m \left((1-p_m) P_m^{\frac{2}{a_b}} + p_m J_m^{\frac{2}{a_b}}\right)}. \tag{7}$$

Proof. See Appendix C. □

Theorem 2 derives the coverage probability when the typical WNE is unable to detect malicious nodes but is capable of associating with WNEs operating in different spectrum bands. We denote this probability by $\hat{\mathcal{C}}$.

Theorem 2. *The coverage probability $\hat{\mathcal{C}}$ in a multi-tier HWN where i) the typical WNE is unable to detect malicious WNEs, ii) access is prioritized across the accessible tiers in $\mathbb{T}$ based on their band of operation and according to the policy $(\mathbb{T}_1, \cdots, \mathbb{T}_B)$, iii) the RSQ thresholds for all tiers in $\mathbb{T}$ are higher than one, and iv) the tier-m WNEs act independently as jammers and black holes with probability p_m and q_m ($m \in \mathbb{M}$), respectively, is given by*

$$\hat{\mathcal{C}} = \sum_{b=1}^{B} \mathcal{C}_b \cdot \Pi_{k=1}^{b-1} \left(1 - \mathcal{A}_k\right) \tag{8}$$

where $\mathcal{C}_b$ and $\mathcal{A}_k$ are derived by Eqs. (1) and (6).

Proof. See Appendix D. □

Theorem 2 provides a *lower performance bound* on the coverage performance of multi-tier HWNs with randomly distributed black hole and jammer nodes, when both the network and the end terminals are fully unable to detect malicious WNEs and thus, employ effective countermeasures. Besides, Theorem 2 can also be used to assess the coverage probability of *different frequency/RAT-based association policies* in the same scenario, or even identify the optimal (frequency/RAT based) association policy through exhaustive search (i.e. by calculating the coverage probability of all feasible policies and employing the one with the highest gain). Notably, since WNEs operating in different spectrum bands do not interfere with each other, the optimal association policy (in terms of coverage probability) can be obtained using Proposition 1.

Proposition 1. *The optimal frequency-based association policy in a multi-tier HWN with randomly distributed jammer and black hole nodes where the typical WNE is unable to detect malicious WNEs, is given by the ordered set of accessible tiers per band according to their coverage probability $\mathcal{C}_b$ in a descending order.*

Proof. It can be proved based on the fact that i) the parameters λ_m, P_m, J_m, p_m, q_m, and γ_m are fixed, and ii) DL communications in different bands are performed independently. □

In contrast to the complexity required to identify the optimal frequency/RAT-based association policy through exhaustive search ($B!$ iterations), Proposition 1 can derive the optimal association policy using B iterations. It should also be noted that Proposition 1 is a simple yet highly-effective *countermeasure* to maximize network coverage in the presence of joint jamming and black hole attacks, when the end terminals are fully unable to detect and avoid malicious WNEs.

V. Numerical Results and Design Guidelines

In this section, we exploit the analytical expressions derived in section IV to assess the performance of DL communications in the practical HWN setup discussed in Section III.D. Accordingly, the system model parameters B, $\mathbb{B}$, M, $\mathbb{M}$ and $\mathbb{T}$ as well as the subsets $\mathbb{M}_b$ and $\mathbb{T}_b$ for $b \in \mathbb{B}$, are valued in line with Section III.D. To highlight the usefulness of the proposed analysis and derive valuable guidelines for the design of robust communications in multi-tier HWNs, we evaluate and compare the coverage probability of the four-tier HWN under three different scenarios of high practical interest.

In the first scenario, termed as the *No-Attack* scenario, we evaluate network coverage in the absence of malicious WNEs (i.e. $p_m = 0$ and $q_m = 0$ for all $m \in \mathbb{M}$). In the second scenario, termed as the *Upper Bound (UB)* scenario, we assume that the typical WNE can perfectly detect and avoid association with malicious WNEs (Section IV.A). In the third scenario, termed as the *No detection* scenario, we consider that the typical WNE is unable to detect malicious WNEs (Section IV.B). Since network performance in the *No detection* scenario strongly depends on the association policy used to prioritize access across the different network tiers, we assess and plot the performance of different association policies that prioritize access among tiers based on their operating frequency.

Note that all RSQ thresholds are assumed to be higher than the unit SIR; thus, there can be up to one WNE exhibiting SIR higher than one in a given spectrum band (Lemma 1). To this end, in the *No detection* scenario, we distinguish the different association policies by using the notation $B = \{b_x, \cdots b_y\}$. This notation corresponds to the ordered set of bands used as the prioritization policy at the typical WNE, where a given band $b \in \mathbb{B}$ is included in the association policy only if the typical WNE has access to at least one of the tiers operating in this band. Unless differently stated, the remainder system model parameters and their values are in line with Table I.

A. On the number of accessible tiers and spectrum bands

In Fig. 2 we assess the coverage probability with respect to the number (and type) of tiers through which the typical WNE can receive DL data (i.e. different setups of $\mathbb{T}$). In the upper histogram, we plot the coverage probability when the typical WNE is capable of receiving DL data from a single network tier (and thus a single band), in the middle histogram when it can receive DL data from two tiers operating in different bands, and in the bottom histogram when it can receive DL data from all tiers in $\mathbb{T} = \{2, 3, 4\}$. Each histogram plots the coverage probability obtained under the *No-Attack* and the *UB* scenarios, as well as the coverage probability obtained by all feasible frequency-based association policies in the *No detection* scenario (malicious WNE cannot be detected).

TABLE I
System Parameters and Their Values

Parameters	**Values**
Path loss exponent per band	$a_1 = 3.2$, $a_2 = 3.5$, $a_3 = 3.8$
Network intensities	$\lambda_1 = 10^{-2}$, $\lambda_2 = 10^{-3}$, $\lambda_3 = 10^{-3.5}$, $\lambda_4 = 10^{-5}$
RSQ thresholds	$\gamma_1 = 2\ (3dB)$, $\gamma_2 = 1.01\ (0.04dB)$, $\gamma_3 = 1.01\ (0.04dB)$, $\gamma_4 = 1.01\ (0.04dB)$
Transmit power of regular/ black hole WNEs (per tier)	$P_1 = 1mW$, $P_2 = 100mW$, $P_3 = 0.5W$, $P_4 = 1W$
Transmit power of jammer WNEs (per tier)	$J_1 = 2mW$, $J_2 = 200mW$, $J_3 = 0.5W$, $J_4 = 1.5W$
Prob. of jamming attacks (per tier)	$p_1 = 0.15$, $p_2 = 0.1$, $p_3 = 0.1$, $p_4 = 0.05$
Prob. of black hole attacks (per tier)	$q_1 = 0.1$, $q_2 = 0.1$, $q_3 = 0.05$, $q_4 = 0.1$

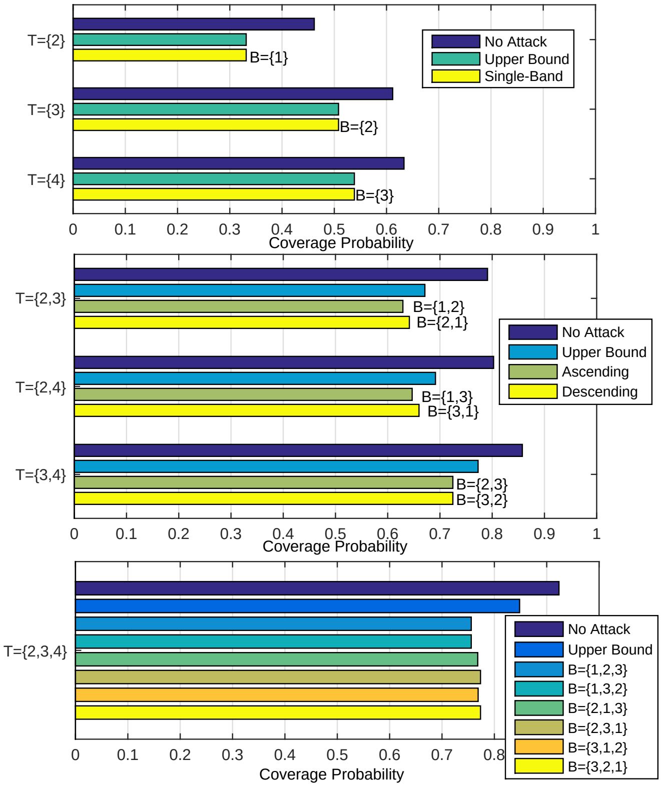


Fig. 2. Coverage probability vs. the set of accessible tiers $\mathbb{T}$

We start our discussions with the upper histogram of Fig. 2. In this histogram, we tag the association policy employed in the *No detection* scenario as *Single-Band*. As expected, the coverage probability for DL communications with a given network tier, as derived by the proposed analysis framework, is not simply given by the probability that the WNEs of that tier are regular (e.g. for $m \in \mathbb{M}$ this probability is calculated by $(1 - p_m - q_m)$). Instead, the derived expressions account for more practical system parameters that include the transmit power, the RSQ thresholds per tier, the density of WNEs across the different tiers, the coexistence of different RATs/tiers in a given band, the openness of a given network tier to jamming and black hole attacks (attack probability - intrusion rate), the set of accessible network tiers (or available RAT interfaces) at the typical WNE, the association policy employed, etc.

In the presence of jamming and black hole attacks, the results in the upper histogram of Fig. 2 imply that network coverage does not depend on the capability of the typical WNE to detect malicious WNEs, or not (i.e. *Upper-Bound* and *Single-Band* performance is equal). This result is in line with intuition if we consider that, even when the typical WNE can detect malicious WNEs, the capability of receiving DL data only from a single tier (and thus band), limits the association options (at the typical WNE) to up to one WNE (satisfying the higher-than-one RSQ threshold), which can be regular, malicious, or even inaccessible (i.e. not part of $\mathbb{T}$). Thus, the employment of more sophisticated countermeasures can be beneficial, only if the typical WNE can utilize different spectrum bands, or RATs. This result further highlights that the use of radio receivers with RSQ threshold requirements lower than the unit SINR (0 dB) would not only increase the association options available at the receiver (i.e. more WNEs would satisfy the RSQ threshold), but would also enhance system robustness against jamming and black hole attacks.

For the given system parameters, the reception of DL data from tier-2 WNEs exhibits the lowest performance (i.e. plots for $\mathbb{T} = \{2\}$) under all scenarios within scope. This result follows from the fact that tier-2 WNEs are assumed to co-utilize the same spectrum band with the low-power yet densely-deployed tier-1 WNEs (Table I). Besides, the system model parameters further imply that tier-2 WNEs are more vulnerable to jamming and black hole attacks (i.e. increased tier-1/tier-2 jamming and tier-2 black hole probabilities). In contrast, higher network tiers exhibit enhanced network coverage (e.g. plots for $\mathbb{T} = \{3\}$, $\mathbb{T} = \{4\}$), due to i) the lower population of WNEs (and thus potential interferes) in the respective tiers (λ_3 and λ_4 lower than λ_2), ii) the increased path loss exponent (thus reduced interference) in the respective bands of operation (a_3 and a_4 higher than a_1), and iii) the reduced probability with which the WNEs act as jammers and black holes in the respective tiers (q_3, q_4, p_3 and p_4 are lower than the respective q_2 and p_2 parameters). The results in the upper histogram of Fig. 2 also indicate that the joint impact of jamming and black hole attacks on network coverage is even more evident when the HWN inherently exhibits a low coverage probability in the absence of malicious WNEs (e.g. compare the *No-Attack* and the *Upper Bound* performance for $\mathbb{T} = \{2\}$ and $\mathbb{T} = \{3\}$).

Let us now turn our attention to the middle histogram of Fig. 2 (data reception from up to two tiers). In this histogram, we distinguish the results of the *No detection* scenario, by terming as *Ascending* the results derived for the association policy giving priority to tiers with lower coverage probability and as *Descending* the results derived for the association policy giving priority to tiers with higher coverage probability (optimal policy - Proposition 1). By comparing the results of the *No-Attack* scenario in the upper and middle histograms of Fig. 2, it can be seen that the utilization of multiple spectrum bands (even using the same RAT interface) significantly increases the coverage probability in the absence of malicious WNEs. Although this performance trend is pretty much expected, the coverage probability is not simply given by the maximum of the coverage probabilities per accessible tier. Instead, it is comparably higher and depends on the number of accessible bands through which the typical WNE can receive DL data. Accordingly, it follows that the proposed analysis framework can be used to assess the performance gains following from the utilization of multiple spectrum bands in regular HWNs.

Moving one step further, when the typical WNE is unable to detect malicious WNEs (*Ascending* and *Descending* scenarios) an inevitable performance degradation is observed as compared to the *No-Attack* and the *Upper Bound* scenarios. The range of this performance degradation strongly depends on the set of accessible tiers, while notable correlation between the network coverage performance and the association policy is shown in the *No detection* scenario results (*Ascending*, *Descending* plots). Besides, the results of Fig. 2 validate our findings in Proposition 1. In more detail, when the typical WNE is unable to detect malicious WNEs, the frequency-based association policy that prioritizes access to tiers with higher coverage probability, i.e. the *Descending* policy, exhibits the optimal performance in all setups of $\mathbb{T}$. For example, when the typical WNE has access to three tiers (bottom histogram), the optimal prioritization policy is given by $B = \{3, 2, 1\}$. For the given system parameters it is shown that, as compared to the *No-Attack* scenario, the typical WNE experiences a performance degradation of up to 10% when it is capable of avoiding association with malicious nodes (*Upper Bound*), and up to 25% when it is fully unable to detect malicious WNEs (*Ascending* policy). This result highlights that the proposed analysis framework can be used to quantify the performance of different frequency-based association policies in the *No detection* scenario, in addition to serving as a reference point for the upper bound performance that can be achieved by the employment of more sophisticated techniques that allow perfect detection of malicious WNEs (*Upper Bound* scenario).

The results of Fig. 2 further indicate that the use of WNEs with limited functional capabilities, in terms of number of utilized spectrum bands and RAT interfaces, can be a limiting factor to the risk management options available to the network administrator as well as to the actions that can be delivered towards protecting critical infrastructures, e.g. for the navigation of autonomous vehicles and unmanned aerial vehicles, or the distant access/control of local cyber-physical equipment. Nonetheless, the derived results also highlight that even the use of simple security countermeasures, which in this paper are based on the prioritization of access across different network tiers and spectrum bands, can be highly effective if properly designed and optimized. The effectiveness of such countermeasures, however, strongly depends on the number of available spectrum bands in the system as well as the density and transmission profile of incumbents in accessible tiers. The development of more sophisticated security countermeasures, allowing perfect detection of malicious behaviors, is still needed to safeguard system robustness and maximize network coverage of HWNs. In this direction, the analysis presented in this paper can be readily used to quantify the effectiveness of future countermeasures, providing specific bounds for the

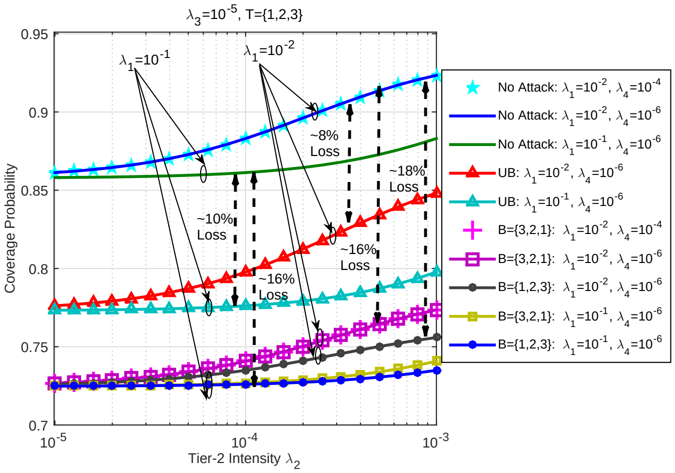


Fig. 3. Coverage probability vs. intensity of tier-2 WNEs

minimum and maximum network coverage that can be attained in the presence of joint jamming and black hole attacks.

B. On the network intensity

Fig. 3 depicts the coverage probability for different network intensities per tier in the four-tier HWN under scope. For the given system parameter values, we observe that the coverage probability is not affected by the density of tier-4 WNEs. This can be easily verified by observing that the coverage plots for $\lambda_4 = 10^{-4}$ (cyan star) and $\lambda_4 = 10^{-6}$ (blue) in the *No-Attack* scenario coincide. The same applies in the presence of malicious nodes for $\lambda_4 = 10^{-4}$ (pink cross) and $\lambda_4 = 10^{-6}$ (magenta square) in the *No detection* scenario (i.e. plots with different B={$\cdots$}). Similar conclusions can be derived for the impact of the tier-3 intensity λ_3, leading us to the conclusion that the coverage probability is not affected by an increase in the intensity of network tiers that are the only incumbents in their band. This trend can be explained as follows. For a given spectrum band, as the density of WNEs operating in-band increases, the signal strength and the interference level increase with the same factor; thus, the observed SINR remains unchanged. This result is consistent with previous studies on the coverage performance of multi-tier networks that assume distinct operating bands across the network tiers [16].

However, different from previous works, Fig. 3 also reveals that this property does not hold when the same spectrum band is (co)utilized by two different network tiers. For example, provided that tier-1 and tier-2 WNEs operate in the same band b_1 and that only tier-2 WNEs are accessible to the typical WNE, an increase of the tier-2 intensity λ_2 is shown to improve the coverage probability. The respective performance improvement strongly depends on the intensity of tiers operating in the same spectrum band, i.e. the coverage probability in Fig. 3 increases rapidly with λ_2 when $\lambda_1 = 10^{-2}$ (red triangle) but slowly when $\lambda_1 = 10^{-1}$ (higher tier-1 intensity). The same set of plots verify that an increase to the intensity of tier-1 WNEs, which are not accessible by the typical WNE yet operate in the same band with tier-2 WNEs, degrades network coverage. Thus, we can conclude that an increase in the intensity of accessible network tiers improves network coverage only if the corresponding intensity value is comparable to that of non-accessible tiers operating in the same band.

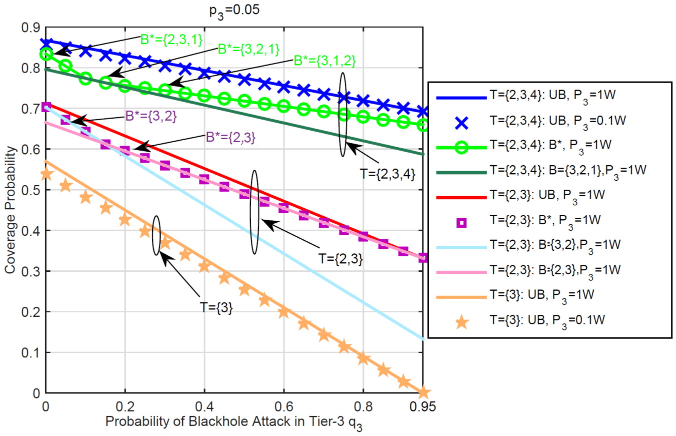


Fig. 4. Coverage probability vs. probability of black hole attacks q_3

Fig. 3 also illustrates that black hole and jamming attacks can lead to notable performance degradation, even when the typical WNE can perfectly detect the malicious WNEs. The corresponding degradation relates to the density of non-accessible tiers, e.g. the coverage probability in the *Upper bound* scenario is reduced by 8% for $\lambda_1 = 10^{-2}$ and by 10% for $\lambda_1 = 10^{-1}$. Once again, the degradation following from jamming and black hole attacks is more evident when the coverage probability is overall lower. This can be readily verified by comparing the performance of the *No-attack* and the *Upper bound* scenarios for $\lambda_1 = 10^{-2}$ and $\lambda_1 = 10^{-1}$. For the given system parameters, we observe a two-fold performance degradation when the typical WNE is unable to detect the malicious WNEs (e.g. for $B = \{3, 2, 1\}$) as compared to the perfect detection (UB) scenario. This result highlights the importance of implementing effective countermeasures that can allow perfect identification of malicious WNEs.

By comparing the performance of the policies $B = \{3, 2, 1\}$ and $B = \{1, 2, 3\}$, it is shown that the proposed countermeasure, which prioritizes access among tiers according to the operating band, exhibits notable performance gains especially when the accessible tiers are characterized by medium to high network intensities (i.e. as λ_2 increases). For the given system parameters, the performance of the optimal prioritization policy (i.e. $B = \{3, 2, 1\}$) is up to 5% lower compared to the *Upper bound* and up to 3% improved compared to the remainder association policies (*No detection* scenario). As will be seen in the sequel, the performance gains of the optimal frequency-based prioritization policy rapidly increase and converge to the ones attained by the *Upper Bound* as the probability of jamming and black hole attacks increases.

C. On the probability of black hole attacks

In Fig. 4 we assess the coverage probability as the probability of black hole attacks in tier-3 increases. For the *No detection* scenario we plot the optimal frequency-based prioritization policy B^* (Proposition 1). Fig. 4 shows that the impact of black hole attacks (in tier-3) is more evident when the typical WNE has access to a lower number of network tiers. In particular, when the typical WNE has access only to tier-3 WNEs ($T = \{3\}$), the coverage probability decreases rapidly with q_3. However, a similar increase of the probability q_3 has a comparably lower impact on the coverage when the typical WNE has access to more tiers, e.g. the performance degradation for $T = \{2, 3, 4\}$ reaches up to 10%. Once again, this result highlights the flexibility and performance gains offered by the employment of multi-band communications in the presence of jamming/black hole attacks, independent of whether end terminals can detect and avoid malicious WNEs.

Fig. 4 also shows that, when the typical WNE is unable to detect black hole WNEs (e.g. plots for $T = \{2, 3, 4\}$: B^* and $B = \{3, 2, 1\}$), network coverage strongly depends on the employed association policy, especially when the probability of black hole attacks increases. It is also worth noting that the optimal prioritization policy changes as the black hole attack probability increases. For example, when the typical WNE has access to tier-2 and tier-3 WNEs ($T = \{2, 3\}$), the prioritization policy $B = \{3, 2\}$ exhibits the optimal performance in the interval $q_3 = [0, 0.17]$, whereas the policy $B = \{2, 3\}$ is optimal in the interval $q_3 = [0.17, 0.95]$. The performance gap between the two prioritization policies increases fast with the probability of black hole attacks, highlighting the importance of model-based adaptation of the association policy in light of the current system status. Similar conclusions are derived for a larger number of accessible tiers $\mathbb{T} = \{2, 3, 4\}$, where the optimal association policy changes two times. For completeness, Fig. 4 includes the performance of the policy $B = \{3, 2, 1\}$ to better highlight the change of the optimal prioritization policy for different q_3 values.

From the discussion above, it readily follows that the analysis presented in this paper can form the basis of comprehensive strategies for safeguarding system robustness against black hole and jamming attacks, through the online estimation of network coverage per band and the model-based adaptation of the association policy at the end terminals (Proposition 1). Besides, the performance of the optimal association policy B^* in the *No detection* scenario is very close to the one attained by the *Upper Bound* under the assumption of perfect detection of malicious WNEs, especially when the probability of black hole attacks is high. This performance trend reveals that in the presence of large-scale attacks, the deployment of low-complexity countermeasures in the challenging scenario where the end terminals are fully unable to detect malicious WNEs, e.g. using frequency-based tier prioritization (Proposition 1), can be adequately effective with the deployment of advanced techniques enabling perfect detection of malicious WNEs.

Fig. 4 further assesses the interplay between the probability of black hole attacks and the transmit power of black hole (or regular) WNEs in the *Upper Bound* scenario. Similar results were derived for the scenarios where the typical WNE is unable to detect malicious WNEs. Notably, even a ten-fold increase of the transmit power P_3 of black hole and regular tier-3 WNEs has little impact on the overall coverage probability for all values of q_3. This result applies both when the typical WNE has access only to tier-3 WNEs ($T = \{3\}$) as well as when it has access to more tiers ($T = \{2, 3, 4\}$). This performance trend follows from the fact that black hole WNEs use the same transmit power with regular WNEs (to avoid detection). Therefore, an increase in the transmit power P_3 not only increases the association probability with regular tier-3 WNEs but also increases the association probability with black hole tier-3 WNEs accordingly. For the given jamming probability $p_3 = 0.1$, this performance coupling is the main reason why the ten-fold increase of the transmit power P_3 has only a small impact on the coverage probability obtained for low-to-medium q_3 values in (4). On the other hand, since tier-3 WNEs are the only occupants of band b_2, the performance gains following from a large increase in the transmit power of black hole and regular WNEs in tiers that exclusively utilize a given spectrum band are very small, while they are also dominated by the probability of black hole attacks.

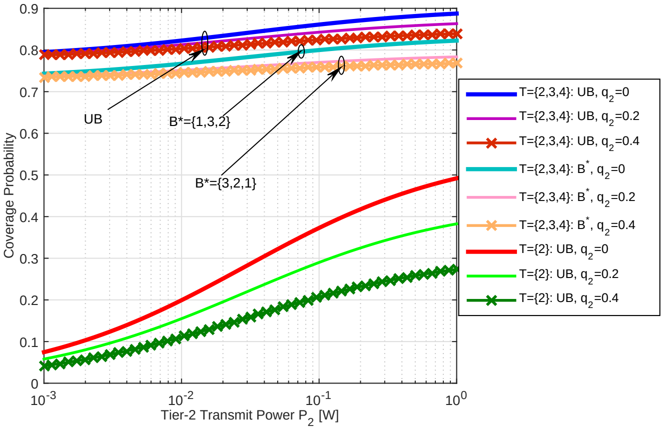


Fig. 5. Coverage probability vs. transmit power P_2

D. On the transmit power of regular and black hole WNEs

In Fig. 5 we assess the coverage probability for different values of the transmit power of black hole and regular WNEs in tier-2. Recall that when the typical WNE has access to a single tier, the performance of the *Upper Bound* and the *No detection* scenarios is the same (Fig. 2). To this end, for $T = \{2\}$, we only include the results for the *Upper Bound* (UB) scenario. Different from Fig. 4, the results of Fig. 5 indicate that an increase in the transmit power of tier-2 black hole and regular WNEs can significantly increase network coverage, especially when the typical WNE has only access to tier-2 (Fig. 5). This performance trend follows from the fact that tier-2 WNEs co-utilize band b_1 with tier-1 WNEs. Accordingly, since the transmit power of tier-1 WNEs remains unchanged (so does the interference level from tier-1 WNEs), even a slight increase of the transmit power P_2 improves the overall coverage probability due to the enhanced DL SIR attained by the (accessible) tier-2 WNEs in band b_1. This performance coupling is not depicted in Fig. 4, given that tier-3 WNEs are the only occupants of band b_2.

As shown in Fig. 5 the rate with which the coverage probability improves (with respect to the transmit power P_2) strongly depends on the number of accessible tiers and the

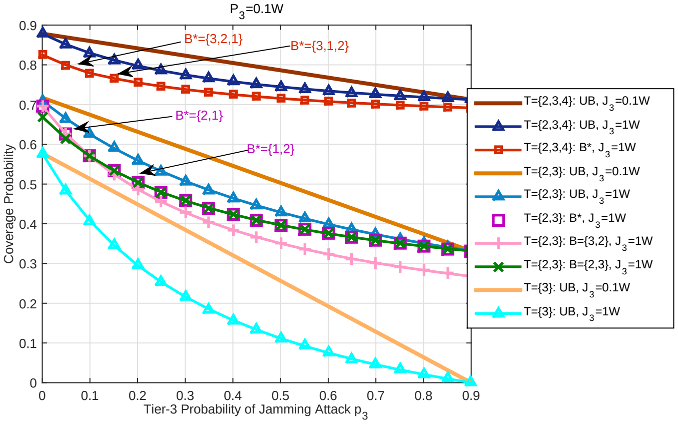


Fig. 6. Coverage probability vs. probability of jamming attacks p_3

probability q_2 of black hole attacks in tier-2. For example, an increase of the transmit power from $P_2 = 10^{-2}$ to $P_2 = 10^{-1}$ Watts almost doubles the coverage probability when the typical WNE has access only to tier-2 WNEs. However, when the typical WNE has access to three networking tiers, the corresponding performance improvement is close to 5%. Since the power consumption at the WNEs is a function of the utilized transmit power, the proposed analytical framework can be used to better comprehend the key performance trade-offs governing the energy-efficiency of WNEs, enabling joint optimizations on the energy consumption, the transmission profile as well as the utilized spectrum bands and RAT interfaces, taking into account the versatile requirements of upper-layer services, e.g. reliability, service availability, system responsiveness [19].

E. On the probability of jamming attacks

In Fig. 6, we investigate the impact of an increasing jamming probability in tier-3 on the coverage performance. Similar to Fig. 4, we examine the coverage probability when the typical WNE has access to a different number of tiers. As expected, the coverage probability increases when the typical WNE has access to a larger number of tiers (i.e. comparison of plots for $T = \{2, 3, 4\}$, $T = \{2, 3\}$ and $T = \{3\}$). Besides, similar to the impact of black hole attacks (Fig. 4), the impact of jamming attacks on network coverage is more evident when the number of accessible ties is low, e.g. performance comparison between $T = \{3\}$ and $T = \{2, 3, 4\}$.

What is more interesting, also highlighting the different structure (and impact) of jamming and black hole attacks, is that an increase in the jamming attack probability degrades network performance with a higher rate as compared to the one observed for a similar increase in the black hole attack probability for the same tier. In more detail, Fig. 4 demonstrates that network coverage reduces almost linearly with the black hole attack probability q_3. The same trend is observed in Fig. 6 when the jammers' power J_3 is close to the transmit power P_3 of regular and black hole WNEs (e.g. for $P_3 = J_3 = 10^{-1}$ Watts). However, when the trasmit power of tier-3 jammer WNEs is higher than that of regular tier-3 WNEs, network coverage degrades fast with an increase in the jamming attack probability (e.g. compare the plots for $T = \{3\}$ for $J_3 = 10^{-1}$ and $J_3 = 10^0$ Watts). This is in line with intuition if we consider that the transmit power of jammers only adds interference to the typical WNEs, whereas an increase in the transmit power of black hole WNEs also comes with an increase in the transmit power of regular WNEs.

Fig. 6 also demonstrates that the performance of the optimal frequency-based association policy $\boldsymbol{B}*$ is very close to the upper performance bound (assuming perfect detection of malicious WNEs), e.g. by comparing the plots for ($T = \{2, 3, 4\}$: UB, $J_3 = 1$W) and ($T = \{2, 3, 4\}$: $B*$, $J_3 = 1$W). The gains offered by this simple countermeasure are even more evident when the typical WNE has access to a lower number of tiers ($T = \{2, 3\}$) and the transmit power of jammers is high ($J_3 = 1$W). In this case, the optimal association policy $\boldsymbol{B}*$ is shown to change from $B* = \{1, 2\}$ to $B* = \{2, 1\}$, when the jamming attack probability surpasses the value of $p_3 = 0.1$. This result further highlights that the complex requirement of achieving perfect detection of malicious WNEs in a multi-tier HWNs can be alleviated if a proper estimation of the coverage probability per band can be achieved (using the closed-form formulas of this work) and an effective frequency-based association policy can be timely deployed (using Proposition 1).

VI. Conclusions

In this paper, we have presented a comprehensive analysis framework to formalize the study of jamming and black hole attacks in multi-tier HWNs. Exact expressions on the coverage performance of such networks have been derived, depending on the capability of end terminals to detect malicious behaviors. In the scenario where end terminals are assumed capable of perfectly detecting malicious nodes, the derived coverage expressions provide an upper performance bound that is tied to the key system parameters affecting network coverage, e.g. network density, set of accessible tiers, utilized spectrum bands. In the scenario where end terminals are unable of detecting malicious nodes, the derived expressions assess network coverage given different association policies that prioritize access across tiers based on their operating spectrum band. The optimal association policy for this scenario has also been derived. Extensive numerical results have quantified the flexibility offered by the utilization of multiple spectrum bands (or RATs) by the end terminals (in light of alleviating jamming and black hole attacks) and have further assessed the performance gap between i) the employment of advanced techniques enabling perfect detection of malicious nodes and ii) the employment of the optimal association policy when the end terminals are totally unable to detect malicious nodes, under different use cases of high practical interest. In future work, we aim to extend the results of our analysis to incorporate potential observation error for the perfect detection scenario as well as to use the derived expressions to model and analyze the performance of the network under more sophisticated DoS attacks that evolve in the time domain.

Appendix

A. Proof of Theorem 1

Assuming that the typical WNE can detect malicious WNEs, the coverage probability in a given band $b \in \mathbb{B}$ is derived by:

$$
\begin{aligned}
\mathcal{C}_b &= P\left[\cup_{\tau\in\mathbb{T}_b, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \\
&\overset{(a)}{=} \sum_{\tau\in\mathbb{T}_b} E\left[\cup_{x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \\
&\overset{(b)}{=} \sum_{\tau\in\mathbb{T}_b} \frac{\int_{\mathbb{R}^2} P\left[\frac{P_x h_x \|\mathbf{x}\|^{a_b}}{\sum_{m\in\mathbb{M}_b}\sum_{y\in\Phi_m} P_y h_y \|\mathbf{y}\|^{-a_b}} > \gamma_\tau\right] \mathrm{d}\mathbf{x}}{\left((1-q_\tau-p_\tau)\lambda_\tau\right)^{-1}} \\
&\overset{(c)}{=} \sum_{\tau\in\mathbb{T}_b} (1-q_\tau-p_\tau)\lambda_\tau \int_{\mathbb{R}^2} P\left[h_x > \frac{\gamma_\tau I(x)}{P_x\|\mathbf{x}\|^{a_b}}\right] \mathrm{d}\mathbf{x} \\
&\overset{(d)}{=} \sum_{\tau\in\mathbb{T}_b} (1-q_\tau-p_\tau)\lambda_\tau \int_{\mathbb{R}^2} E_{I(x)}\left[e^{\frac{\gamma_\tau I(x)}{P_x\|\mathbf{x}\|^{a_b}}}\right] \mathrm{d}\mathbf{x} \qquad (9)
\end{aligned}
$$

where (a) follows from the fact that up to one WNE can exhibit SIR higher than one per band (Lemma 1); thus, the events $\mathbf{1}(SIR(x) > \gamma_\tau)$ are disjoint, (b) follows from the Campbell-Mecke theorem [20] and the SIR definition in (2), (c) follows by rearranging (b) and the definition in (3), and (d) follows from the assumption of Rayleigh fading. Notice that the expectation in (9) corresponds to the Laplace transform of the interference caused by the remainder tier-τ WNEs (malicious or not). However, since the locations of WNEs are independent of the location of the typical WNE, the interference level $I(x)$ is immaterial to the actual location of the typical WNE $\mathbf{x}$. In view of that, in the sequel we let $s = \frac{\gamma_\tau}{P_x\|\mathbf{x}\|^{a_b}}$ and omit the argument from $I(x)$. Accordingly, the expectation in (9) is given by the Laplace transform:

$$
\mathcal{L}_I[s] = E_I\left[\exp\left(-s\sum_{m\in\mathbb{M}_b}\sum_{y\in\Phi_m\setminus\{x\}} P_y h_y \|\mathbf{y}\|^{-a_b}\right)\right] \qquad (10)
$$

$$
\begin{aligned}
&\overset{(a)}{=} \Pi_{m\in\mathbb{M}_b} E_I\left[\Pi_{y\in\Phi_m\setminus\{x\}} \exp\left(-sP_y h_y\|\mathbf{y}\|^{-a_b}\right)\right] \\
&\overset{(b)}{=} \Pi_{m\in\mathbb{M}_b} E_{\Phi_m}\left[\Pi_{y\in\Phi_m\setminus\{x\}} E_h\left[\exp\left(-sP_y h_y\|\mathbf{y}\|^{-a_b}\right]\right)\right] \\
&\overset{(c)}{=} \Pi_{m\in\mathbb{M}_b} E_{\Phi_m\setminus\{\Phi_{mj}\}}\left[\Pi_{y\in\Phi_m\setminus\{x,\Phi_{mj}\}} \frac{1}{1+sP_m\|\mathbf{y}\|^{-a_b}}\right] \\
&\qquad\qquad \cdot E_{\Phi_{mj}}\left[\Pi_{\mathbf{z}\in\Phi_{mj}} \frac{1}{1+sJ_m\|\mathbf{z}\|^{-a_b}}\right] \\
&\overset{(d)}{=} \Pi_{m\in\mathbb{M}_b} e^{-(1-p_m)\lambda_m \int_{\mathbb{R}^2}\left(1-\frac{1}{1+sP_m\|\mathbf{y}\|^{-a_b}}\right)\mathrm{d}\mathbf{y}} \\
&\qquad\qquad \cdot e^{-p_m\lambda_m \int_{\mathbb{R}^2}\left(1-\frac{1}{1+sJ_m\|\mathbf{z}\|^{-a_b}}\right)\mathrm{d}\mathbf{z}} \\
&\overset{(e)}{=} \Pi_{m\in\mathbb{M}_b} e^{-\frac{2\pi^2\csc\left(\frac{2\pi}{a_b}\right)}{a_b} s^{\frac{2}{a_b}} \lambda_m\left((1-p_m)P_m^{\frac{2}{a_b}} + p_m J_m^{\frac{2}{a_b}}\right)} \\
&\overset{(f)}{=} e^{-\frac{2\pi^2\csc\left(\frac{2\pi}{a_b}\right)}{a_b} s^{\frac{2}{a_b}} \sum_{m\in\mathbb{M}_b}\lambda_m\left((1-p_m)P_m^{\frac{2}{a_b}} + p_m J_m^{\frac{2}{a_b}}\right)} \qquad (11)
\end{aligned}
$$

where (a) follows by considering that the locations of WNEs belonging to different tiers are independent, (b) by taking into account that the fading powers at the WNEs are independent of their locations (Rayleigh fading), (c) by using the moment generating function of the (exponentially distributed) fading power and by dividing the point process Φ_m into two mutually independent point processes based on the transmit power of the WNEs (i.e. jammers transmit with J_m and regular/black hole WNEs with P_m), (d) by using the Campbell-Mecke Theorem for the independent processes Φ_{mj} and $\Phi_m\setminus\{\Phi_{mj}\}$, (e) by solving the integrals in (d) and merging the exponential expressions, and (f) by rearranging (e). The proof of Theorem 1 concludes by substituting (11) in (9) and solving the integral. Note that $sinc\left(\frac{2\pi}{a_b}\right) = \frac{\sin\left(\frac{2\pi}{a_b}\right)}{\left(\frac{2\pi}{a_b}\right)}$.

B. Proof of Corollary 1

Assuming that the typical WNE can detect malicious WNEs, the coverage probability $\mathcal{C}$ can be derived as follows:

$$
\begin{aligned}
\mathcal{C} &= P\left[\cup_{\tau\in\mathbb{T}, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \qquad (12) \\
&\overset{(a)}{=} 1 - P\left[\cap_{b\in\mathbb{B}, \tau\in\mathbb{T}_b, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) \leq \gamma_\tau)\right] \\
&\overset{(b)}{=} 1 - \Pi_{b\in\mathbb{B}}\left(1 - P\left[\cup_{\tau\in\mathbb{T}_b, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right]\right) \\
&\overset{(c)}{=} 1 - \Pi_{b\in\mathbb{B}}\left(1 - \mathcal{C}_b\right) \qquad (13)
\end{aligned}
$$

where (a) follows by taking the complement of (12) and by using $\mathbb{T} = \cup_{b\in\mathbb{B}}\mathbb{T}_b$, (b) follows by considering that DL communications across different spectrum bands are performed independently and by taking the complement of the respective probability, and (c) follows by the definition of the probability $\mathcal{C}_b$. By using the results of Theorem 1 we conclude the proof.

C. Proof of Corollary 2

Given that the typical WNE is unable to detect malicious WNEs, the association probability $\mathcal{A}_b$ in a given spectrum band $b \in \mathbb{B}$ is derived by:

$$
\begin{aligned}
\mathcal{A}_b &= P\left[\cup_{\tau\in\mathbb{T}_b, x\in\Phi_\tau} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \qquad (14) \\
&= \sum_{\tau\in\mathbb{T}_b} E\left[\cup_{x\in\Phi_\tau\setminus\Phi_{\tau j}} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \\
&\quad + \sum_{\tau\in\mathbb{T}_b} E\left[\cup_{x\in\Phi_{\tau j}} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \qquad (15)
\end{aligned}
$$

where Eq. (15) follows from Lemma 1 (up to one WNE can exhibit SIR higher than one per band, leading to disjoint coverage events). The derivations continue in Eqs. (16) and (17) (next page), where Eq. (16) follows from the Campbell-Mecke theorem and by considering that the transmit power of tier-τ regular/black hole WNEs is fixed at P_τ while the transmit power of tier-τ jammer WNEs is fixed at J_τ ($\tau \in \mathbb{T}_b$), and Eq. (17) follows from the assumption of Rayleigh fading and by noticing that the resulting expectation corresponds to the Laplace transform of the interference at point $\mathbf{x}$. Thus, by using (11) and solving the integral in (17) we reach to (7).

D. Proof of Theorem 2

Let $A_b = \cup_{\tau\in\mathbb{T}_b, x\in\Phi_\tau}\mathbf{1}(SIR(x) > \gamma_\tau)$ denote the event where at *least one WNE (regular or not)* operating in band $b \in \mathbb{B}$ satisfies the RSQ threshold for its tier and let

$$= \sum_{\tau\in\mathbb{T}_b}(1-p_\tau)\lambda_\tau\int_{\mathbb{R}^2}P\left[\frac{P_\tau h_x\|\mathbf{x}\|^{a_b}}{\sum_{m\in\mathbb{M}_b}\sum_{y\in\Phi_m}P_y h_y\|\mathbf{y}\|^{-a_b}}>\gamma_\tau\right]\mathrm{d}\mathbf{x}+\sum_{\tau\in\mathbb{T}_b}p_\tau\lambda_\tau\int_{\mathbb{R}^2}P\left[\frac{J_\tau h_x\|\mathbf{x}\|^{a_b}}{\sum_{m\in\mathbb{M}_b}\sum_{y\in\Phi_m}P_y h_y\|\mathbf{y}\|^{-a_b}}>\gamma_\tau\right]\mathrm{d}\mathbf{x} \tag{16}$$

$$= \sum_{\tau\in\mathbb{T}_b}\left((1-p_\tau)\lambda_\tau\int_{\mathbb{R}^2}\mathcal{L}_I\left[\frac{\gamma_\tau}{P_\tau\|\mathbf{x}\|^{a_b}}\right]\mathrm{d}\mathbf{x}\right)+\sum_{\tau\in\mathbb{T}_b}\left((1-p_\tau)\lambda_\tau\int_{\mathbb{R}^2}\mathcal{L}_I\left[\frac{\gamma_\tau}{J_\tau\|\mathbf{x}\|^{a_b}}\right]\mathrm{d}\mathbf{x}\right) \tag{17}$$

$C_b = \cup_{\tau\in\mathbb{T}_b r, x\in\Phi_\tau}\mathbf{1}(SIR(x)>\gamma_\tau)$ denote the event where *at least one regular* WNE in band b satisfies the RSQ threshold for its tier. Also, let $\bar{A}_b$ denote the event where there exists no WNE in band b to belong in the *accessible* tiers in $\mathbb{T}_b$ and satisfy the RSQ threshold for its tier at the same time, and let $\hat{C}$ denote the coverage event (i.e. successful association of the typical WNE with a regular WNE) when i) the typical WNE is unable to detect malicious WNEs and ii) it prioritizes access among the tiers in $\mathbb{T}$ according to the policy $(\mathbb{T}_1,\cdots,\mathbb{T}_B)$.

We now focus on the coverage event $\hat{C}$. Given the association policy $(\mathbb{T}_1,\cdots,\mathbb{T}_B)$, the typical WNE is in coverage if i) there exists a *regular* WNE in $\mathbb{T}_1$ satisfying the RSQ threshold γ_1, or if ii) there is no WNE (*regular or not*) in $\mathbb{T}_1$ to satisfy γ_1, but there exists a *regular* WNE in $\mathbb{T}_2$ satisfying γ_2, or if iii) there is no WNE (*regular or not*) in $\mathbb{T}_1\cup\mathbb{T}_2$ to satisfy the RSQ threshold of its tier, but there exists a *regular* WNE in $\mathbb{T}_3$ satisfying γ_3, and so on. Given that i) the locations of WNEs operating in different bands are independent (i.e. Φ_m for $m\in\mathbb{M}$ are mutually independent), ii) DL communications across different bands in $\mathbb{B}$ are performed independently, and iii) up to one WNE can exhibit SIR higher than one in a given band (Lemma 1), it readily follows that the coverage event is structured as follows $\hat{C}=\cup_{b=1}^{B}\left(\left(\cap_{k=1}^{b-1}\bar{A}_k\right)\cup C_b\right)$.

At this point, it is important to note that the events $\bar{A}_b$ and C_b are disjoint. This can be easily verified by noticing that the event $\bar{A}_b$ refers to the absence of an accessible WNE (regular or not) to operate in band b and satisfy the RSQ threshold for its tier, whereas the event C_b refers to the existence of at least one regular WNE to operate in band b and satisfy the RSQ threshold for its tier. In view of that, we can derive the coverage probability $\hat{\mathcal{C}}=P[\hat{C}]$ as follows:

$$\hat{\mathcal{C}}\overset{(a)}{=}P\left[\cup_{b=1}^{B}\left(\left(\cap_{k=1}^{b-1}\bar{A}_k\right)\cup C_b\right)\right]$$

$$\overset{(b)}{=}P\left[C_1\cup\left(\bar{A}_1\cap\left(C_2\cup\left(\bar{A}_2\cap\left(\cdots\left(C_{B-1}\cup\left(\bar{A}_{B-1}\cap C_B\right)\right)\right)\right)\right)\right)\right]$$

$$\overset{(c)}{=}\mathcal{C}_1+(1-\mathcal{A}_1)\cdot(\mathcal{C}_2+(1-\mathcal{A}_2)\cdot(\cdots(\mathcal{C}_{B-1}+(1-\mathcal{A}_{B-1}\cdot\mathcal{C}_B))))$$

$$\overset{(d)}{=}\sum_{b=1}^{B}\mathcal{C}_b\cdot\Pi_{k=1}^{b-1}\left(1-\mathcal{A}_k\right)$$

where (b) follows by developing (a) to unions and intersections of disjoint events, (c) by taking into account that i) the events $\mathcal{C}_b$ are mutually independent for all $b\in\mathbb{B}$, ii) the events $\bar{\mathcal{A}}_b$ are mutually independent for all $b\in\mathbb{B}$, and iii) the events $\mathcal{C}_b$ and $\bar{\mathcal{A}}_b$ are disjoint by construction, and (d) by developing the products of (c) and factorizing them in a single sum of products. The proof completes using Theorem 1/Corollary 2.

References

[1] Ericsson, ”Ericsson mobility report”, *Technical Report*, June 2017.

[2] Technical Specification (TS) 38.300 V15.3.1, 3GPP, July 2018

[3] R. Tourani, S. Misra, T. Mick and G. Panwar, ”Security, Privacy, and Access Control in Information-Centric Networking: A Survey”, *IEEE Commun. Surv. & Tut.*, vol. 20, no. 1, pp. 566-600, Q1 2018.

[4] T. Ibragimov, O. Kupreev, E. Badovskaya, A. Gutnikov, ”DDoS attacks in Q2 2018”, Report by Kaspersky Lab in securelist.com, June 2018.

[5] Y. Liu, M. Dong, K. Ota and A. Liu, ”ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks”, *IEEE Tran. on Inform. Forensics and Security*, vol. 11, no. 9, pp. 2013-2027, Sept. 2016.

[6] T. Shu, M. Krunz and S. Liu, ”Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes”, *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941-954, July 2010.

[7] S. Petridou, S. Basagiannis and M. Roumeliotis, ”Survivability Analysis Using Probabilistic Model Checking: A Study on Wireless Sensor Networks”, *IEEE Systems*, vol. 7, no. 1, pp. 4-12, March 2013.

[8] Y. Guan, X. Ge, ”Distributed Secure Estimation over Wireless Sensor Networks against Random Multichannel Jamming Attacks”, *IEEE Access*, vol. 5, pp. 10858-10870, 2017.

[9] J. Zhu, Y. Zou and B. Zheng, ”Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks”, *IEEE Access*, vol. 5, pp. 5313-5320, 2017.

[10] H. Zhang, P. Cheng, L. Shi and J. Chen, ”Optimal DoS Attack Scheduling in Wireless Networked Control System”, *IEEE Trans. on Control Systems Techn.*, vol. 24, no. 3, pp. 843-852, May 2016

[11] Hongmei Deng, Wei Li and D. P. Agrawal, ”Routing security in wireless ad hoc networks,” *IEEE Commun.*, vol. 40, no. 10, pp. 70-75, Oct 2002.

[12] J. Ponniah, Y. C. Hu and P. R. Kumar, ”A System-Theoretic Clean Slate Approach to Provably Secure Ad-Hoc Wireless Networking”, *IEEE Trans. on Control of Network Sys.*, vol. 3, no. 2, pp. 206-217, June 2016.

[13] D. Hoang, D. Niyato, P. Wang and D. I. Kim, ”Performance Analysis of Wireless Energy Harvesting Cognitive Radio Networks Under Smart Jamming Attacks”, *IEEE Trans. on Cognitive Commun. and Netw.*, vol. 1, no. 2, pp. 200-216, June 2015.

[14] S. Amuru, H. Dhillon, R. Buehrer, ”On Jamming Against Wireless Networks”, *IEEE Trans. on Wirel. Commun.*, vol. 16, no. 1, pp. 412-428, Jan. 2017.

[15] D. Berger, F. Gringoli, N. Facchi, I. Martinovic, J. Schmitt, ”Friendly Jamming on Access Points: Analysis and Real-World Measurements”, *IEEE Trans. on Wirel. Commun.*, vol. 15, no. 9, pp. 6189-6202, 2016.

[16] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, ”Modeling and Analysis of K-tier Downlink Heterogeneous Cellular Networks”, *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550-560, Mar. 2012.

[17] D. Xenakis, L. Merakos, M. Kountouris, N. Passas, C. Verikoukis, ”Distance Distributions and Proximity Estimation given Knowledge of the Heterogeneous Network Layout”, *IEEE Trans. on Wirel. Commun.*, vol.14, no.10, pp.5498-5512, Oct. 2015.

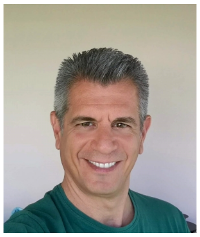
[18] D. Xenakis, N. Passas, L. Merakos, C. Verikoukis, ”Mobility Management for Femtocells in LTE-Advanced: Key Aspects and Survey of Handover Decision Algorithms”, *IEEE Comm. Surv. & Tut.*, vol.16, no.1, pp.64-91, Q1 2014.

[19] ITU-R, “Minimum requirements related to technical performance for IMT-2020 radio interface(s)”, Report ITU-R M.2410-0, Nov 2017.

[20] D. Stoyan, W. Kendall, and J. Mecke, Stochastic Geometry and its Applications, 2nd ed., *John Wiley and Sons*, 1996.

Anastasia Tsiota received the BSc degree from the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Greece, in 2012 with a scholarship from the Papadakis Foundation. In 2015, she received the M.Sc. degree in Data Networks and Communication Systems from the same department with scholarship from the A. Onassis Foundation. Mrs. Tsiota is currently a PhD candidate in the National and Kapodistrian University of Athens, in the field of reliable data communications in multi-tier wireless networks. She has participated in various EU and Greek-funded research projects. Her current research interests include network security for multi-tier networks, incentive engineering technologies for wireless data transfer and stochastic modeling/analysis of 5G mobile data networks.

Dionysis Xenakis received the Ph.D. degree from the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Greece, in 2014. He has participated in numerous EU-funded projects and co-authored more than 30 peer-reviewed journal and conference papers. He has served as TPC member and chair top-tier IEEE conferences, while he has been reviewer to high-ranking IEEE journals in Computer Science and Data Networks. Dr. Xenakis is recipient of the Special Grant & Support program by the Onassis Foundation. His current research interests lie in the design and analysis of 5G and beyond mobile data network technologies with the emphasis given in multi-access edge computing and distributed ledger technologies.



Nikos Passas received his Diploma (honors) from the Department of Computer Engineering, University of Patras, Greece, and his Ph.D. degree from the Department of Informatics and Telecommunications, University of Athens, Greece, in 1992 and 1997, respectively. He is currently a member of the teaching staff in the Department of Informatics and Telecommunications of the University of Athens, and a group leader of the Green, Adaptive and Intelligent Networking (GAIN) research group inside the department. Over the years, he has participated and coordinated a large number of national and European research projects. Dr. Passas has served as a guest editor and technical program committee member in prestigious magazines and conferences, such as IEEE Wireless Communications Magazine, Wireless Communications and Mobile Computing Journal, IEEE Vehicular Technology Conference, IEEE PIMRC, IEEE Globecom, etc. He has published more than 140 papers in peer-reviewed journals and international conferences. His research interests are in the area of mobile network architectures and protocols. He is particularly interested in quality of service provision for wireless networks, medium access control, and mobility management.

Lazaros Merakos received the Diploma in electrical and mechanical engineering from the National Technical University of Athens, Greece, in 1978, and the M.S. and Ph.D. degrees in electrical engineering from the State University of New York, Buffalo, in 1981 and 1984, respectively. Dr. Merakos was on the faculty of the Electrical Engineering and Computer Science Department, University of Connecticut (1983-1986), on the faculty of the Electrical and Computer Engineering Department, Northeastern University, Boston (1986-1994) and has served as Director of the Communications and Digital Signal Processing Research Center, Northeastern University (1993–1994). Since 1994, he has been a Professor in the Department of Informatics and Telecommunications and Director of the Communication Networks Laboratory, where he has led several EU funded projects that have shaped European R&D in the area of mobile networking. His research interests are in the area of network technologies, services and applications. He has authored more than 280 papers in the above areas. Dr. Merakos is chairman of the board of the Greek Universities Network(GUNet).