Jamming and Black Hole Attacks in the Smart Grid with Perfect Detection of Malicious Nodes

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

***Abstract*—In this paper, we focus on the impact of blackhole and jamming attacks on the coverage probability experienced by communication-enabled smart grid equipment. In a black hole attack, a subset of communication-enabled nodes appear as regular nodes of the smart grid without forward the packets of associated nodes to their intended destination. In a jamming attack, part of the smart grid nodes transmit at high power in order to disrupt and interfere the communications of regular nodes of the network. A key contribution of our work is a new methodological approach for stochastic modeling of the smart grid equipment locations that allows the derivation of closed-form expressions describing the negative impact following from the joint employment of blackhole and jamming attacks in the smart grid. The analytical expressions allows to derive valuable insights for robust and smart grid specific protocol design under the SMART-NRG architecture.**

***Index Terms*—Smart grid, jamming attack, black hole attack.**

I. Introduction

At present, much effort is being made to install smart meters (SMs) into millions of homes across Europe. European regulations require member nations to ensure that 80% of residential households will be fitted with a smart meter by 2020 [1]. With the help of the densely deployed SMs, the today's energy grid will be modernized to be a more intelligent, responsive, efficient, and environmentally sustainable system of systems, widely known as the smart grid [2]. Since the energy monitoring and management processes, including the so-called demand-response cycle, involve the exchange of sensitive information on the energy consumption of the end consumers, their behavioral changes as well as technical specifications of the machinery installed at the consumers' premises, the security of the smart grid is a critical issue.

Due to the nature of the power grid, its main constituting parts have been long viewed as isolated and treated independently in terms of security measures from external attacks. However, since the smart grid aims to provide new services, further relying on the communication infrastructure, the increased number of connections with the communication infrastructure, and in particular with the internet, has the potential to increase the security risks and number of inadvertent attacks. Thus, the security of the smart grid, and in particular of the metering infrastructure, is of critical importance. In this work, we focus on the performance of the smart grid that is under the joint impact of jamming attacks (parasitic interference) and black hole attacks.

The jamming attacks are made by an entity widely known as a jammer that aims to disrupt wireless communications by creating interference during both the emission and the reception of packets. The jammer typically emits a strong wireless signal continuously aiming to cover a wireless channel and hinder the reception of over-the-air packets. The jamming attacks degrade network performance as they can result in a denial of service (DoS), posing a primary security threat to wireless networks. Current literature includes two basic types of jamming attacks: the non-reactive and the reactive attack [3]. Non-reactive jammers transmit interference signals by following their own strategies, while reactive jammers transmit interfering signals only when they become aware of any activity in a wireless channel.

On the other hand, black hole attacks are more complicated as they occur when a set of network nodes are reprogrammed (by someone malicious) to block (or reject) the packets they receive (or produce) rather than forward them to their destination [4]. Therefore, any information entering the coverage area of black hole nodes, a.k.a. the black hole area, is typically discarded (and further processed to extract sensitive information). Black hole attacks are easy to place and may compartmentalize the network, undermining the effectiveness of two-way end-to-end information flow in the smart grid.

In the Smart Grid, the jamming and black hole attacks may aim either interrupt the localized exhange of information between the smart metering infrastructure and the individual energy measurement sensors in the consumer premises, or disrupt the communications between the smart meters and the local controller / data aggregator that is responsible for collecting measurements and sending instructions related to the operation of the smart Grid in a particular area [stef]. For example, a competitor may delay (or prevent) the collection of smart meter indications and insert the pricing signals transmitted in real time to the last mile of communication between the utility and the end consumer service [5].

In this work, we propose a new stochastic model tailored to smart grid architectures similar to that of the SMART-NRG project and derive closed-form expressions describing the negative impact of joint blackhole and jamming attacks on the coverage probability experienced by the communication-enabled nodes. We subsequently assess the coverage probability of the SMART-NRG architecture and provide valuable insights on how to optimize its performance in the presence of black hole and jamming attacks.

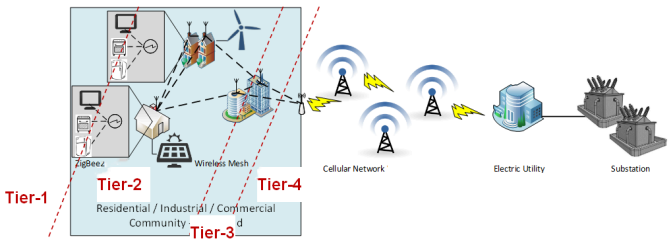

Fig. 1. The four-tier SMART-NRG reference archicture [6]

II. System Model

We consider the four-tier SMART-NRG reference architecture that is tailored to the exchange of measurement and control messages in the Smart Energy Grid [6] (Fig. 1). The first tier includes low-power sensors that measure and control the energy consumption of end devices located at the consumers' premises. The second tier is composed by smart meters (SMs) that forward control data to the tier-1 WNEs (low-power sensors) located at the consumers' premises and collect localized measurement data produced by the same set of tier-1 WNEs. The third tier includes local data aggregation points (LDAPs) that monitor and control the energy consumption of an entire neighborhood, whereas the fourth tier includes cellular base stations that act as intermediate relays between the the utility operator, the LDAPs, and the SMs.

Without loss of generality, we consider that each tier consists of wireless networking elements (WNEs) that serve similar communication purposes and support the same RAT. Moreover, we term the WNEs belonging to the m-th tier as tier-m WNEs ($m \in \mathbb{M} = \{1, 2, 3, 4\}$). Their locations are assumed to be distributed according to a homogeneous PPP Φ_m of intensity λ_m in the Euclidean plane with $m \in \mathbb{M}$. The locations of the WNEs belonging to different tiers are assumed to be mutually independent. In addition, the WNEs belonging to different tiers may operate in different frequency bands, utilize diverse transmit powers, support different data rates and be characterized by different spatial densities. Nonetheless, all WNEs belonging to the same tier are assumed to operate in the same frequency band and, in the absence of malicious WNEs, to utilize the same (fixed) transmit power. In the sequel, we denote by P_m the transmit power of all regular (i.e. non-malicious) WNEs belonging to tier-m.

We further focus on the performance of downlink (DL) communications of a tagged WNE, termed as the typical WNE, that is not part of the smart grid infrastructure modeled by the processes Φ_m ($m \in \mathbb{M}$). Since the WNEs of the same networking tier utilize the same frequency band, in the following, we consider the use of B different frequency bands in the entire network with $B \leq 4$ (i.e. WNEs belonging to different tiers may operate in the same frequency band). We also denote by $\mathbb{B}$ the set of utilized frequency bands and by $\mathbb{M}_b \subseteq \mathbb{M}$ the set of networking tiers (i.e. their identifiers) that operate in a given frequency band $b \in \mathbb{B}$. Note that the sets $\mathbb{M}_b$ are disjoint by construction. Radio transmissions in a given frequency band $b \in \mathbb{B}$, are assumed to be governed by the same path loss exponent a_b.

Also, let $\mathbb{T} \subseteq \mathbb{M}$ denote the set of *accessible tiers* (i.e. their identifiers) through which the typical WNE can receive its DL data. We further divide the set $\mathbb{T}$ into B disjoint sets based on the utilized frequency band of each networking tier $\tau \in \mathbb{T}$ and denote by $\mathbb{T}_b \subseteq \mathbb{M}_b$ the set of tiers that are accessible by the typical WNE and operate in a given band $b \in \mathbb{B}$, where $\mathbb{T} = \cup_{b \in \mathbb{B}} \mathbb{T}_b$. We further consider that, for a given tier $\tau \in \mathbb{T}$, the minimum required received signal quality (threshold) for successful reception of DL data at the typical WNE is fixed and is denoted by γ_τ. For analytical tractability, we also assume that the signal quality threshold of all tiers is higher than one (i.e. $\gamma_\tau > 1 \forall \tau \in \mathbb{T}$) and focus our analysis in interference-limited networks where the successful reception of data is mainly affected by the interference caused by the WNEs operating in the same frequency band (i.e. the impact of thermal noise at the receiver is negligible).

To better understand the system model parameters and how they can be adapted in practice, let us consider (only as an example) that the typical WNE can receive DL data in three different ways: i) by employing MTC with other SMs in proximity using Wi-Fi communications in a given band b_1, ii) by associating with the LDAP responsible for its neighborhood using Wi-Fi communications in a given band b_2, and iii) by utilizing the cellular network infrastructure operating in a given band b_3. Assuming that the low-power sensors (tier-1 WNEs) transmit in the frequency band b_1, the system model parameters for the particular SM of interest (typical WNE) are given as follows: $M = 4$, $\mathbb{M} = \{1, 2, 3, 4\}$, $B = 3$, $\mathbb{B} = \{b_1, b_2, b_3\}$, $\mathbb{M}_1 = \{1, 2\}$, $\mathbb{M}_2 = \{3\}$, $\mathbb{M}_3 = \{4\}$, $\mathbb{T} = \{2, 3, 4\}$, $\mathbb{T}_1 = \{2\}$, $\mathbb{T}_2 = \{3\}$, $\mathbb{T}_3 = \{4\}$.

Let us now focus on the modeling of the jammers and black holes. In the sequel, we assume that the WNEs of a given tier $m \in \mathbb{M}$ act as jammers or black holes at random and independently from the remainder WNEs with probability p_m and q_m, respectively, where $0 \leq p_m + q_m \leq 1$. We further consider that all the tier-m jammer WNEs transmit at a fixed transmit power that we denote by J_m. In practice, we expect J_m to be the maximum allowable transmit power for the tier-m WNEs with $J_m \geq P_m$; however, the subsequent analysis applies for all values of J_m. Different from the tier-m jammer WNEs, we consider that all the tier-m WNEs acting as black holes use the same transmit power P_m with the regular WNEs aiming to avoid detection. Nonetheless, the black hole WNEs are considered to disrupt the forwarding of DL data towards the WNEs that associate with them.

Since the tier-m WNEs act maliciously at random and independently, the locations of the tier-m jammer WNEs can be described by the PPP Φ_{mj} with intensity $p_m \cdot \lambda_m$, the locations of the tier-m black hole WNEs by the PPP Φ_{mb} with intensity $q_m \cdot \lambda_m$, and the locations of the regular tier-m WNEs by the PPP Φ_{mr} with intensity $(1-p_m-q_m) \cdot \lambda_m$, where $\Phi_m = \Phi_{mj} \cup \Phi_{mb} \cup \Phi_{mr}$. Notably, this modeling approach also applies when the jammer and the black hole WNEs are modeled as external WNEs.

We now turn our attention to the performance of the typical WNE in terms of *coverage probability*, by taking into account the joint presence of (random) jamming and black hole attacks in the smart grid. In particular, aiming to derive upper performance bounds for the coverage probability in such networks, 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 minimum required threshold for its tier. By letting $SIR(x)$ denote the SIR of the WNE x, we formally define the *coverage probability* as follows:

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

Since the WNEs of the four-tier SMART-NRG architecture may operate in different frequency bands, the estimation of $SIR(x)$ strongly depends on the operating frequency band of the WNE x. In the sequel, we consider that the fading power between the typical WNE and a tagged WNE $x \in \cup_{m\in\mathbb{M}}\Phi_m$, which we denote by h_x, is subject to Rayleigh fading, i.e. the random variables (RVs) h_x are independent and identically distributed with (unitary) exponential distribution. For notational convenience, we also denote by P_y the transmit power of a given WNE $y \in \cup_{m\in\mathbb{M}}\Phi_m$ and by $\|y\|$ its physical distance from the typical WNE. Accordingly, for a given WNE x that operates in the frequency band b and belongs to an accessible tier in $\mathbb{T}$, we define the $SIR(x)$ as follows:

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

Note that the denominator of (2) can be further analyzed based on the transmit power of the different types of WNEs per tier. In the sequl, we denote the total interference from WNEs operating in the same frequency band with the tagged WNE x by $I(x)$. In Lemma 1, we summarize an interesting application of a well-known result from [7].

Lemma 1. *For a given frequency band $b \in \mathbb{B}$, there can be up to one WNE belonging to the -tier smart grid infrastructure and exhibits received signal quality higher than one.*

Proof. Lemma 1 is a direct application of Lemma 1 in [7]. We omit the proof for brevity. □

III. Performance Analysis

In this section, we focus on the performance of DL communications in the SMART-NRG smart grid architecture with joint jamming and black hole attacks. In particular, we derive upper performance bounds for the coverage probability of a tagged WNE of interest (the typical WNE) that is not necessarily part of the smart grid infrastructure but is capable of receiving its data from multiple tiers of the smart grid. We further consider that the typical WNE can detect the malicious WNEs and avoid association with them. In future work we plan to genaralize our derivations in the scenario where the typical WNE is unable to detect the malicious WNEs. Note that the following expressions can be readily generalized under more generic smart grid architectures. In the sequel, we consider that the typical WNE is in coverage if there exists at least one regular WNE that belongs to the set of accessible tiers in $\mathbb{T}$ and exhibits a SIR higher than the minimum required threshold for its tier.

Theorem 1. *Let $\mathcal{C}_b$ denote the coverage probability for DL communications in a given frequency band $b \in \mathbb{B}$. Given that the typical WNE can detect the malicious WNEs and that the received signal quality threshold for all tiers in $\mathbb{T}_b$ is higher than one, the coverage probability is given by:*

$$\mathcal{C}_b = \frac{\sin\left(\frac{2\pi}{a_b}\right)\cdot\sum_{\tau\in\mathbb{T}_b}\left(\frac{2\pi}{a_b}\right)\cdot\lambda_\tau(1-q_\tau-p_\tau)P_\tau^{\frac{2}{a_b}}\gamma_\tau^{-\frac{2}{a_b}}}{\sum_{m\in\mathbb{M}_b}\lambda_m\left((1-p_m)P_m^{\frac{2}{a_b}}+p_m J_m^{\frac{2}{a_b}}\right)}. \quad (3)$$

Proof. Given that the typical WNE can detect and avoid association with the malicious WNEs, the coverage probability in a given frequency band $b \in \mathbb{B}$ can be derived as follows:

$$\begin{aligned}
\mathcal{C}_b &= P\left[\cup_{\tau\in\mathbb{T}_b, x\in\Phi_{\tau r}}\mathbf{1}(SIR(x)>\gamma_\tau)\right] \\
&\overset{(a)}{=} \sum_{\tau\in\mathbb{T}_b} E\left[\cup_{x\in\Phi_{\tau r}}\mathbf{1}(SIR(x)>\gamma_\tau)\right] \\
&\overset{(b)}{=} \sum_{\tau\in\mathbb{T}_b}(1-q_\tau-p_\tau)\lambda_\tau\int_{\mathbb{R}^2} P\left[h_x > \frac{\gamma_\tau I(x)}{P_x\|\mathbf{x}\|^{a_b}}\right]\mathrm{d}\mathbf{x} \\
&\overset{(c)}{=} \sum_{\tau\in\mathbb{T}_b}(1-q_\tau-p_\tau)\lambda_\tau\int_{\mathbb{R}^2} E_{I(x)}\left[e^{\frac{\gamma_\tau I(x)}{P_x\|\mathbf{x}\|^{a_b}}}\right]\mathrm{d}\mathbf{x} \quad (4)
\end{aligned}$$

where (a) follows from Lemma 1 (i.e. up to one WNE can exhibit SIR higher than one in a given frequency band - the events $\mathbf{1}(SIR(x) > \gamma_\tau)$ are disjoint), (b) follows from the Campbell-Mecke theorem [8] and the SIR definition in (2), and (c) follows from the assumption of Rayleigh fading. Notice that the expectation in (4) corresponds to the Laplace transform of the interference caused by all the remainder tier-τ WNEs (malicious or not). However, since the locations of the WNEs are independent of the location of the typical WNE, the interference level $I(x)$ does not depend on 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 (4) is given by the following Laplace transform:

$$\mathcal{L}_I[s] = E_I\left[\exp\left(-s\sum_{m\in\mathbb{M}_b}\sum_{y\in\Phi_m\setminus\{x\}} P_y h_y\|\mathbf{y}\|^{-a_b}\right)\right] \quad (5)$$

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

$$\overset{(f)}{=} \quad e^{\left(-\frac{2\pi^2 \csc\left(\frac{2\pi}{a_b}\right)}{a_b} s^{\frac{2}{a_b}} \sum_{m\in\mathbb{M}_b} \lambda_m \left((1-p_m)P_m^{\frac{2}{a_b}} + p_m J_m^{\frac{2}{a_b}}\right)\right)} \tag{6}$$

where (a) follows since the locations of WNEs belonging to different tiers are independent, (b) since 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 using the Campbell-Mecke Theorem for the independent processes Φ_{mj} and $\Phi_m \backslash \{\Phi_{mj}\}$ (i.e. jammer WNEs transmit with J_m, whereas regular and black hole WNEs with P_m), (d) by solving the integrals and merging the exponential expressions, and (e) by rearranging (e). The proof concludes by substituting (6) in (4) and solving the integral. □

Let us now turn our attention to the challenging scenario where the typical WNE can receive its DL data from WNEs that operate in different frequency bands. In this scenario, there can exist more than one (and up to B) regular WNEs that satisfy the requirement of received signal quality higher than one. In Theorem 2, we derive the coverage probability when the typical WNE can detect the malicious WNEs and receive DL data from WNEs operating in different frequency bands.

Theorem 2. *The coverage probability for DL communications in a multi-tier HWN where i) the typical WNE can detect the malicious WNEs and has access to the set of tiers in $\mathbb{T}$, ii) the received signal quality threshold for all tiers in $\mathbb{T}$ is higher than one and iii) the tier-m WNEs act at random and independently as jammers and black holes with probability p_m and q_m ($m \in \mathbb{M}$), respectively, is given by:*

$$\mathcal{C} = 1 - \Pi_{b\in\mathbb{B}} \left(1 - \mathcal{C}_b\right). \tag{7}$$

Proof. Given that the typical WNE can detect and avoid association with malicious WNEs, the coverage probability $\mathcal{C}$ can be derived as follows:

$$\begin{aligned} \mathcal{C} &= P\left[\cup_{\tau\in\mathbb{T}, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right] \\ &\overset{(a)}{=} 1 - P\left[\cap_{b\in\mathbb{B}, \tau\in\mathbb{T}_b, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) \leq \gamma_\tau)\right] \\ &\overset{(b)}{=} 1 - \Pi_{b\in\mathbb{B}} \left(1 - P\left[\cup_{\tau\in\mathbb{T}_b, x\in\Phi_{\tau r}} \mathbf{1}(SIR(x) > \gamma_\tau)\right]\right) \end{aligned} \tag{8}$$

where (a) follows by taking the complement of (8) and by using $\mathbb{T} = \cup_{b\in\mathbb{B}} \mathbb{T}_b$ and (b) follows by considering that the DL communications across the different frequency bands are performed independently and by taking the complement of the respective probability. The proof concludes by using the definition of the coverage probability $\mathcal{C}_b$ and Theorem 1. □

Note that the expressions in Theorems 1 and 2 can be readily used to assess the coverage probability in regular smart grids that are not subject to jamming and black hole attacks (i.e. for $q_m = 0$ and $p_m = 0$ with $m \in \mathbb{M}$).

IV. Numerical Results and Discussion

In this section, we exploit the derived expressions to assess the performance of DL communications under the SMART-NRG architecture in the presence of joint jamming and black hole attacks. We focus on the performance of a particular smart meter of interest (the typical WNE) that can receive DL data by using direct MTC with other SMs in proximity (tier-2 WNEs), by associating with the LDAP responsible for its neighborhood (tier-3 WNEs), or by exploiting the cellular network infrastructure (tier-2 WNEs). We further evaluate and compare the coverage probability under two scenarios of high practical interest. In the first scenario, termed as the *No-Attack* scenario, we evaluate the coverage probability of the SMART-NRG network in the absence of cyberphysical attacks (i.e. $p_m = 0$ and $q_m = 0$ for all $m \in \mathbb{M}$). In the second scenario, termed as the *Joint-Attack* scenario, we evalute the coverage probability in the presence of joint random jamming and black hole attacks assuming that the typical WNE can perfectly identify and avoid association with the malicious WNEs. Unless differently stated, the system model parameters are given in Table IV.

Parameter	**Value**
Frequency bands	$B = 3$, $\mathbb{B} = \{1, 2, 3\}$
Path loss exponent per band	$a_1 = 3.2$, $a_2 = 3.5$, $a_3 = 3.8$
Network tiers	$M = 4$, $\mathbb{M} = \{1, 2, 3, 4\}$
Network intensity (per tier)	$\lambda_1 = 10^{-2}$, $\lambda_2 = 10^{-3}$, $\lambda_3 = 10^{-3.5}$, $\lambda_4 = 10^{-5}$
Tier groups per band	$\mathbb{M}_1 = \{1, 2\}$, $\mathbb{M}_2 = \{3\}$, $\mathbb{M}_3 = \{4\}$
Accessible tiers	$T = 3$, $\mathbb{T}_1 = \{2\}$, $\mathbb{T}_2 = \{3\}$, $\mathbb{T}_3 = \{4\}$, $\mathbb{T} = \{2, 3, 4\}$
Received signal quality thresholds (per tier)	$\gamma_1 = 2$ $(3dB)$, $\gamma_2 = 1.01$ $(0.04dB)$, $\gamma_3 = 1.01$ $(0.04dB)$, $\gamma_4 = 1.01$ $(0.04dB)$
Transmit power of regular and 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)	$J_1 = 2mW$, $J_2 = 200mW$, $J_3 = 0.5W$, $J_4 = 1.5W$
Probability of jamming attacks (per tier)	$p_1 = 0.15$, $p_2 = 0.1$, $p_3 = 0.1$, $p_4 = 0.05$
Probability of black hole attacks (per tier)	$q_1 = 0.1$, $q_2 = 0.1$, $q_3 = 0.05$, $q_4 = 0.1$

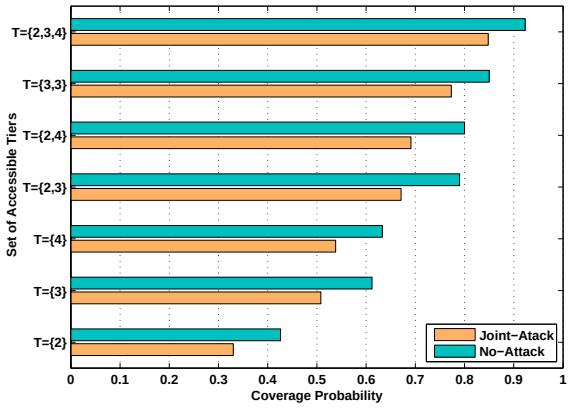

Fig. 2. Coverage probability vs. Set of accessible tiers $\mathbb{T}$

In Fig. 2 we investigate the coverage probability when the typical WNE can receive DL data from different tiers of the HWN. Fig. 2 reveals that the coverage probability for DL communications with a given networking tier (or frequency

band) is not simply given by the probability with which the accessible WNEs of that tier (or band) are regular, e.g. for a tagged tier $m \in \mathbb{M}$ this probability is given by $(1-p_m-q_m)$. Instead, the coverage probability is additionally affected by the spatial distribution of WNEs as well as the minimum received signal quality threshold required at the typical receiver. Besides, as indicated by the results in Fig. 2, the requirement of satisfying a minimum received signal quality threshold can significantly lower the probability of successful reception of DL data at the typical WNE. The results of our analysis provide a tractable framework that jointly accounts for the performance limitations following from the design of radio trasceivers, in addition to providing quantitative results on the coverage probability experienced by multi-mode mobile terminals in multi-tier smart grids open to jamming and black hole attacks.

For the set of system parameters under scope, we also observe that the employment of MTC with the tier-2 WNEs exhibits the lowest performance (upper histogram for $\mathbb{T} = \{2\}$). This result follows from the co-utilization of the same frequency band ($b = 1$) by the densely-deployed tier-1 and tier-2 WNEs. However, this result also follows from the increased probability with which the WNEs of the respective networking tiers act as jammers or black holes (Table IV) that is chosen so as to effectively model the openess of the respective networking equipment to the end consumers of a real-life Smart Grid. In contrast, the reception of DL data from WNEs that belong to higher networking tiers (e.g. plots for $\mathbb{T} = \{3\}$, $\mathbb{T} = \{4\}$) experiences enhanced network coverage due to the reduced interference level in the respective tiers (i.e. lower network intentisites λ_3 and λ_4), the increased path loss exponent governing the communication in the respective frequency bands (i.e. a_3 and a_4), as well as the lower probability with which the WNEs of the respective tiers act as jammers or black holes (Table IV). The results in Fig. 2 also indicate that the impact of joint jamming and black hole attacks (on the coverage probability) is even more evident when the network inherently exhibits a low coverage probability in the absence of malicious WNEs (e.g. No-Attack and Joint-Attack scenarios for $\mathbb{T} = \{2\}$ and for $\mathbb{T} = \{2\}$).

Fig. 2 also reveals that the utilization of multiple frequency bands (even by using the same RAT interface) can significantly increase the coverage probability in the absence of malicious WNEs (e.g. access to more than one tiers). Although this performance is expected, note that (when the typical WNE can utilize multiple frequency bands) the coverage probability is not simply given by the maximum of the coverage probabilities per accessible tier as someone would have expected. Instead, the corresponding coverage probability can be comparably higher and strongly depends on the number of accessible networking tiers as well as the number of utilized frequency bands.

Let us now focus on the scenarios where malicious WNEs disrupt the communications of the typical WNE (i.e. Joint-Attack scenarios). The performance of the Joint-Attack scenario under all feasible combinations of accessible sets (all of which are plotted in 2) is inevitably lower to that experienced in the No-Attack scenario. The range of the respective degradation strongly depends on the set of accessible tiers and for the given set of system model values, this performance degradation varies between 10% and 25% depending on the number of accessible tiers. Notably, the performance degradation due to the joint presence of jammers and black holes is inversely proportional to the number of accessible tiers. To conclude, the support of different RATs and multiple frequency bands can play a key role in safeguarding the robustness of communications experienced by the today's mobile terminals.

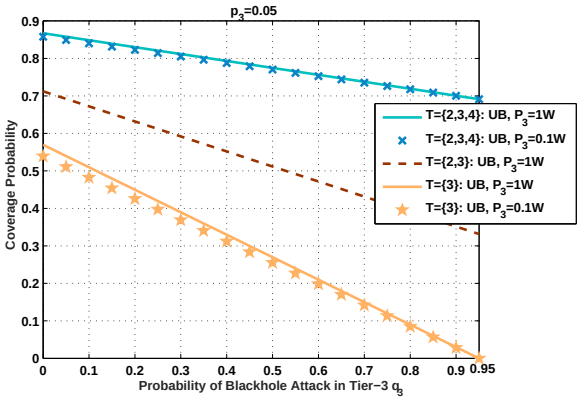

Fig. 3. Coverage probability vs. probability of black hole attacks q_3

A. *On the impact of the probability of black hole attacks*

Fig. 3 shows the coverage probability when the black hole probability of malicious behavior in the third tier increases. Recall that in the case of blackhole attacks, the malicious nodes transmit at the same power as regular nodes. Also, note that the sum of blackhole and jamming attack probabilities for a given tier is lower than one. To better comprehend the impact of black hole attacks in the Smart Grid, in Fig. 3 we plot the coverage probability given different combinations (and number) of accessible tiers. As expected, in the presence of attacks, the coverage probability (assuming perfect detection of malicious behaviors in the smart grid) increases when the typical WNE has access to more tiers (compare curves for $T = \{2,3,4\}$ $T = \{2,3\}$ and $T = \{3\}$). For example, although the increase of the probability q_3 can even eliminate the coverage probability when the typical WNE can receive DL data only from the third tier (curves $T = \{3\}$), the same increase of the probability q_3 has comparably lower impact if the typical WNE has access to all three levels of $T = \{2,3,4\}$. This follows from the fact that when the typical WNE can access a higher number of accessible tiers is less vulnerable to blackhole attacks in a specific tier.

Let us now turn our attention on how the transmit power of blackhole (and regular) nodes per tier affect the successful reception of data at the typical WNE. Notably, even a ten-fold increase of the transmit power of tier-3 black holes and regular nodes leaves the coverage probability roughly unaffected. This

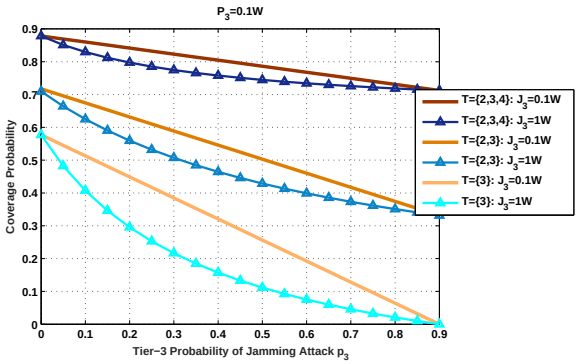

Fig. 4. Coverage probability vs. probability of jamming attacks p_3

effect is observed independent of the number of tiers (or frequency bands) that the typical WNE can access. This mainly follows from the fact that an increase of the transmit power of black hole WNEs also implies a corresponding increase of the transmit power of regular nodes (by construction). As a result, the marginal improvement observed for a higher transmit power P_3 mainly follows from the lower probability with which the typical WNE will associate with a jammer WNE. This gain is greatly reduced when the density of malicious WNEs increases significantly and becomes comparable to (or greater than) the density of regular WNEs. Consequently, an increase of the transmit power of black holes (and thus of the regular NWEs) in frequency bands where there is no network coexistence across the different tiers, can slightly increase the coverage probability. Nonetheless, this gain is almost eliminated when the probability of blackhole attack increases in the respective tier.

B. On the impact of the probability of jamming attacks

In Fig. 4 we depict the coverage probability in the Smart Grid for different values of the jamming attack probability p_3 in the third tier. Similar to the case of blackhole attacks (Fig. 3), an increased number of accessible tiers enhances the coverage probability experienced by the typical WNE. Moreover, the negative impact of an increased probability of malicious jamming behavior on the coverage probability is more evident when the typical WNE has access to less tiers of the Smart Grid. This phenomenon is even more evident when the typical WNE has access only to the specific tier of interest (i.e. the third tier) of the Smart Grid (bottom curves). Nonetheless, what is of particular interest and highlights the different nature of jamming and blackhole attacks, is that the coverage probability decreases at a higher rate for an increasing jamming probability as compared to the respective decrease experienced on the coverage probability for the same increase in the probability of black hole attacks.

More specifically, if we compare the plots in Figs. 3 and 4, we can observe that and increase of the q_3 blachole attack probability reduces the coverage probability in a linear fashion. The same can be said for a similar increase of the jamming attack probability p_3 in the scenario where the transmit power of jammer WNEs is equal to that of black hole and regular WNEs (i.e. $J_3 = P_3 = 0.1W$). However, although the increase in the transmit power P_3 of blackhole nodes does not particularly affect the coverage probability (Fig. 3), a similar incrase of the transmit power J_3 of jammers reduces at an almost exponentially rate the coverage probability (Fig. 4). This can be readily observed, by comparing the curves $T = 3$ for the two different transmit powers $J_3 = 0.1W$ and $J_3 = 1W$. This effect can be explained if we consider that the increase in the transmit power of jammers only adds interference signal quality, even when a frequency band is only utilized by WNEs belonging to a specific tier. Notably, the propsoed analytical framework is capable of assessing and quantifying such relations in the context of the smart grid.

V. Conclusions

In this paper, we have developed a novel analytical framework to assess the coverage probability in smart grid networks that are under the impact of joint black hole and jamming attacks. To better understand practical aspects of our analysis, we have chosen the SMART-NRG smart grid architecture to derive useful design guidelines for secure and robust design of communication protocols in the smart grid. In future work, we intend to account for the clustered distribution of smart grid equipment in the consumers' premises [9] and consider scenarios where the smart grid WNEs are unable to perfectly detect malicious behaviors in the network.

Acknowledgment

This research has been funded by the European Commission as part of the SMART-NRG project (Grant number 612294).

References

[1] European communications, M2M beyond connectivity, Q3 2012 issue.
[2] V. C. Gungor et al., Smart grid technologies: Communication technologies and standards, IEEE Trans. Industrial Informatics, Nov. 2011.
[3] Z. Lu, W. Wang, and C. Wang, Hiding traffic with camouflage: Minimizing message delay in the smart grid under jamming, in IEEE INFOCOM, 2012.
[4] S. Misra, K. Bhattarai, G. Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE International Conference on Communications (ICC), June 2011.
[5] H. Liu, Y. Chen, M. C. Chuah, J. Yang, "Towards self-healing smart grid via intelligent local controller switching under jamming", 2013 IEEE Conference onCommunications and Network Security (CNS), pp.127,135, Oct. 2013.
[6] S. Tennina, D. Xenakis, M. Boschi, M. Di Renzo, F. Graziosi, and C. Verikoukis, "A Modular and Flexible Network Architecture for Smart Grids", Ad Hoc Now 2015, July 2015, Greece.
[7] 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.
[8] D. Stoyan, W. Kendall, and J. Mecke, Stochastic Geometry and its Applications, 2nd ed., John Wiley and Sons, 1996.
[9] D. Xenakis, L. Merakos, M. Kountouris, N. Passas, and 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.