Distributed Network Secrecy

Jemin Lee, *Member, IEEE*, Andrea Conti, *Senior Member, IEEE*, Alberto Rabbachin, *Member, IEEE*, and Moe Z. Win, *Fellow, IEEE*

***Abstract*—Secrecy is essential for a variety of emerging wireless applications where distributed confidential information is communicated in a multilevel network from sources to destinations. Network secrecy can be accomplished by exploiting the intrinsic properties of multilevel wireless networks (MWNs). This paper introduces the concept of distributed network secrecy (DNS) and develops a framework for the design and analysis of secure, reliable, and efficient MWNs. Our framework accounts for node spatial distribution, multilevel cluster formation, propagation medium, communication protocol, and energy consumption. This research provides a foundation for DNS and offers a new perspective on the relationship between DNS and network lifetime.**

***Index Terms*—Distributed network secrecy, self-organizing wireless networks, stochastic geometry, energy consumption, fading channels, performance evaluation.**

I. Introduction

NETWORK SECRECY is a key enabler for various applications in which wireless nodes communicate confidential information to monitoring units (monitors). Example applications include industrial logistics, blue force tracking, and vital-sign acquisition. Confidential information is generally gathered by scattered sensors and communicated to monitors via hierarchical networking, forming a multilevel wireless network (MWN).

In many applications where sensors are equipped with a limited energy supply (e.g., a battery), its efficient utilization is needed to increase the network lifetime. Typically, this is accomplished via self-organization of nodes into clusters at each level [1]–[5]. In this context, the communication confidentiality relies on distributed network secrecy (DNS), which accounts for confidentiality of all active links in the self-organizing MWN.

Contemporary wireless security systems, based on cryptographic primitives, generally ignore the spatial distribution of nodes and the physical properties of wireless environments. This conventional approach can be complemented at the physical layer by exploiting intrinsic properties of a wireless network such as channel and node characteristics [6]–[10].

In the context of physical-layer security, the secrecy capacity has been studied considering fading [11]–[13], multiple access [14]–[16], interference or artificial noise [17]–[19], eavesdropping collusion [20]–[22], and point-to-point diversity communications [23]–[25]. Secret-key generation at the physical-layer using common sources, such as reciprocal wireless channels, has been investigated in [26]–[30]. In addition, secrecy in clustered or multi-hop networks has been investigated in [31]–[33]. However, most of these works ignore the spatial distributions of legitimate and eavesdropping nodes, and relative node positions are important for network secrecy.

A widely used model to represent the node spatial distribution in wireless networks is the Poisson point process (PPP) [34]–[47]. The PPPs have been used to analyze the connectivity of wireless networks with secrecy [48]–[50]. Recently, it has been shown that network interference can benefit network secrecy [51], [52]. However, DNS of self-organizing MWNs has not been established yet, impeding the design of networks capable of offering both communication confidentiality and energy efficiency.

We envision a scenario involving a legitimate self-organizing MWN and an eavesdropping MWN. The former is composed of spatially distributed legitimate nodes aiming to confidentially and efficiently communicate information to a monitor. The latter is composed of spatially distributed eavesdropping nodes aiming to intercept the information flowing in the legitimate network. We introduce the concept of DNS for MWNs and define a new performance metric, namely the *DNS throughput*, to determine the confidential throughput of MWNs. Starting from the observation that the network configuration optimal for DNS may not be the best for energy efficiency, we characterize the relationship between DNS and network lifetime. This enables us to determine the role of multilevel network configuration on secrecy and lifetime, as well as to establish energy-efficient MWNs with DNS.

In this paper, we provide a foundation for DNS in a variety of MWN configurations. The key contributions of the paper can be summarized as follows:

- we introduce the DNS concept and define the DNS throughput in scenarios composed of multilevel legitimate network and eavesdropping network;
- we develop a framework, for the design and analysis of wireless networks with DNS, that accounts for node spatial distribution, multilevel cluster formation, propagation medium, communication protocol, and energy consumption;
- we quantify the DNS throughput and characterize the

Manuscript received September 15, 2012; revised March 10, 2013. This research was supported, in part, by the National Science Foundation under Grant CCF-1116501, by MIT Institute for Soldier Nanotechnologies, by the FP7 European project CONCERTO (Grant Agreement 288502), by the European Commission Marie Curie International Outgoing Fellowship under Grant 2010-272923, and by Korean National Research Foundation under Grants NRF-2011-220-D00076 and NRF-2011-357-D00167. The material in this paper was presented, in part, at the IEEE International Conference on Communications, Budapest, Hungary, June 2013.

J. Lee, A. Rabbachin, and M. Z. Win are with the Massachusetts Institute of Technology (MIT), 77 Massachusetts Avenue, Cambridge, MA 02139 USA (e-mail: jmnlee@mit.edu, rabalb@mit.edu, moewin@mit.edu).

A. Conti is with the University of Ferrara, Via Saragat 1, 44122 Ferrara, ITALY (e-mail: a.conti@ieee.org).

Digital Object Identifier 10.1109/JSAC.2013.130920.

relationship between DNS and network lifetime in self-organizing MWNs.

This work embraces stochastic geometry, probability theory, and communication theory to assess the DNS and the network lifetime for a variety of MWN configurations.

The remainder of this paper is organized as follows: Sec. II describes the network configuration and provides the statistical characterization of received signal-to-noise ratios (SNRs). Section III introduces the DNS concept and Sec. IV analyzes the DNS in fading channels. Section V presents a case study and quantifies DNS performance. Finally, conclusions are given in Sec. VI.

Notation: The notation used throughout the paper is reported in Table I.

II. Multilevel Wireless Networks

In this section, we describe the legitimate and eavesdropping network configurations, provide the statistical characterization of the received SNRs, and derive the network lifetime for an MWN.

A. Multilevel Network Configuration

We consider a scenario composed of a legitimate MWN for gathering and communicating spatiotemporal information as well as an eavesdropping MWN aiming to intercept such information. Legitimate and eavesdropping nodes are randomly scattered in space according to homogeneous PPPs $\mathbf{\Pi}_\ell$, $\mathbf{\Pi}_\mathrm{e} \in \mathbb{R}^d$ with spatial densities λ_ℓ and λ_e, respectively. The goal of legitimate nodes is to communicate their observed data confidentially to monitors. We refer to the entire operation of information gathering via scattered sensors, transmission through MWN, and reception at a monitor as a round.[1] In each round, legitimate nodes self-organize themselves in an MWN: a node is assigned to a level l with probability $\beta^{(l)}$ for $l = L, L-1, \cdots, 1$ where $\sum_{l=1}^{L} \beta^{(l)} = 1$. Therefore, the position of nodes in a level l changes from round to round.

The self-organizing MWN can be seen as a hierarchical network with multiple levels (see, e.g., Fig. 1). In each level $l = L, L-1, \cdots, 1$, the legitimate and the eavesdropping networks are defined as follows:

1) The lth-level legitimate network is composed of nodes that collect and process the information sent by nodes in level $l+1 \leq L$, and transmit them together with their observed information to some nodes in level $l-1$ (monitors are in level 0). By the thinning property [53], the distribution of nodes in level l follows a homogeneous PPP $\mathbf{\Pi}_\ell^{(l)}$ with spatial density $\lambda_\ell^{(l)} = \beta^{(l)}\lambda_\ell$ such that $\sum_{l=1}^{L} \lambda_\ell^{(l)} = \lambda_\ell$.
2) The lth-level eavesdropping network is composed of non-colluding eavesdropping nodes, which attempt to intercept the information transmitted from legitimate nodes in level l. The distribution of eavesdropping nodes in level l follows a homogeneous PPP $\mathbf{\Pi}_\mathrm{e}^{(l)}$ with spatial density $\lambda_\mathrm{e}^{(l)}$ such that $\sum_{l=1}^{L} \lambda_\mathrm{e}^{(l)} = \lambda_\mathrm{e}$.

[1]The monitored environment and the node distribution in a network are considered invariant within a round.

TABLE I
Notations Used Throughout the Paper

Notation	Definition
$\mathbf{\Pi}_\ell$	PPP for legitimate node distribution
$\mathbf{\Pi}_\mathrm{e}$	PPP for eavesdropping node distribution
$\lambda_\ell^{(l)}$	Spatial density of legitimate nodes in level l
$\lambda_\mathrm{e}^{(l)}$	Spatial density of eavesdropping nodes in level l
L	Number of network levels
$\beta^{(l)}$	Probability for a legitimate node to be in level l
T	Symbol time [sec]
W	Communication bandwidth [Hz]
N_0	One-sided power spectral density of AWGN
α	Pathloss exponent
$D_{\mathbf{x},\mathbf{Y}}$	Distance between node positions at $\mathbf{x}$ and $\mathbf{Y}$
$h_{\mathbf{x},\mathbf{Y}}$	Fading level in the link between node positions $\mathbf{x}$ and $\mathbf{Y}$
r_l	Radius of supporting area (cluster) of a node in level $l-1$
b_g	Generated bits per node in a round
b_s	Secret bits per node in a round
s_l	Average number of transmitted symbols/round/node in level l
R_ℓ	Data rate
R_s	Secrecy rate
E_charged	Fully-charged energy of node battery
$E_\mathrm{b}^{(l)}$	Average transmitted energy/bit/node in level l
Δ_l	Energy ratio $E_\mathrm{b}^{(l)}/E_\mathrm{b}^{(L)}$
$\zeta_\ell^{(l)}$	Received SNR by a legitimate node in level $l-1$
$\zeta_\mathrm{e}^{(l)}$	Received SNR by an eavesdropping node in level l
$\check{\zeta}_\ell$	Required SNR at a legitimate receiver
$\check{\zeta}_\mathrm{e}$	Required SNR at an eavesdropper
$\overline{\mathcal{V}}$	Complement of an event $\mathcal{V}$
$\overline{\mathcal{V}}$	Complement of a set $\mathcal{V}$
$\mathcal{B}_\mathbf{X}(r)$	Ball in $\mathbb{R}^d$ of radius r centered at $\mathbf{X}$
$B(r)$	Volume of $\mathcal{B}_\mathbf{X}(r)$
$\mathbb{E}\{\cdot\}$	Statistical expectation
$\mathbb{P}\{\cdot\}$	Probability
$\overline{F}_\mu(\cdot)$	Complementary cumulative distribution function of μ
$\vartheta_1 \wedge \vartheta_2$	Conjunction of events ϑ_1 and ϑ_2
$p_\mathrm{t}^{(l)}$	Probability of transmission at level l
$p_\mathrm{c}^{(l)}$	Probability of not having collision at level l
$p_\mathrm{r}^{(l)}$	Probability of successful reception at level l
$p_\mathrm{e}^{(l)}$	Probability of unsuccessful eavesdropping at level l
N_round	Average number of rounds per node during its lifetime
ρ_ds	DNS throughput

Remark 1: The above network configuration represents scenarios in which eavesdropping nodes are organized in multiple layers (e.g., due to limited intercepting capabilities). However, our framework can be easily adapted to the case where all eavesdropping nodes aim to intercept legitimate transmissions at each level.

After self-organization, the information flows within the MWN as follows. Each node in level l associates with a node in level $l-1$ to form clusters. Each cluster consists of all nodes in level l associated with the same node, referred to as gateway node (GN), in level $l-1$. Nodes in a cluster communicate their

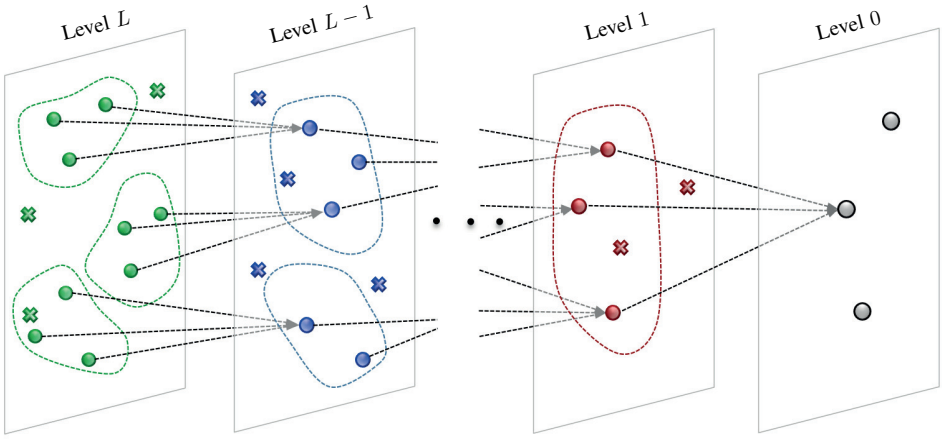


Fig. 1. An example of a legitimate MWN with L levels in the presence of an eavesdropping network (circles are legitimate nodes and crosses are eavesdropping nodes).

observed data to the GN, chosen according to the following probabilistic association rule (PAR). For a node in level l at $\mathbf{x}$, all nodes in level $l-1$ within the ball $\mathcal{B}_{\mathbf{x}}(r_l) \in \mathbb{R}^d$ of radius r_l centered at $\mathbf{x}$, with volume $B(r_l) = |\mathcal{B}_{\mathbf{x}}(r_l)|$, can potentially serve as a GN. Thus $\mathcal{G}_{l-1}(\mathbf{x}) = \mathbf{\Pi}_{\ell}^{(l-1)} \cap \mathcal{B}_{\mathbf{x}}(r_l)$ is the random set of all potential GNs for a node in level l at $\mathbf{x}$.[2] If $|\mathcal{G}_{l-1}(\mathbf{x})| \neq 0$, a GN is selected with equal probability from $\mathcal{G}_{l-1}(\mathbf{x})$ and is represented by the random variable $\mathbf{G}(\mathbf{x})$.[3] If $|\mathcal{G}_{l-1}(\mathbf{x})| = 0$, there is no GN and data collected by a node in level l at $\mathbf{x}$ will be lost.

Legitimate transmitters do not have channel knowledge of legitimate and eavesdropping links. Nodes at different levels communicate using different resources (e.g., different frequency bands or time slots) to avoid inter-level interference, while nodes belonging to the same level share the communication resources according to an intra-level medium access control (MAC) protocol.[4]

We now give a lemma for the derivation of DNS and energy consumption.

Lemma 1: For two independent homogeneous PPPs $\mathbf{\Pi}_u, \mathbf{\Pi}_v \in \mathbb{R}^d$ with densities λ_u and λ_v, respectively, the following property holds

$$\mathbb{E}_{\mathbf{\Pi}_u,\mathbf{\Pi}_v}\left\{\sum_{\mathbf{X}\in\mathbf{\Pi}_u\cap\mathcal{A}} g(\mathbf{X},\mathbf{\Pi}_v)\right\} = \lambda_u \int_{\mathcal{A}} \mathbb{E}_{\mathbf{\Pi}_v}\{g(\boldsymbol{\omega},\mathbf{\Pi}_v)\}\, d\boldsymbol{\omega} \tag{1}$$

where $\mathcal{A}$ is a bounded space with volume $|\mathcal{A}|$. When the process $g(\boldsymbol{\omega},\mathbf{\Pi}_v)$ is stationary in $\boldsymbol{\omega} \in \mathbb{R}^d$, (1) leads to

$$\mathbb{E}_{\mathbf{\Pi}_u,\mathbf{\Pi}_v}\left\{\sum_{\mathbf{X}\in\mathbf{\Pi}_u\cap\mathcal{A}} g(\mathbf{X},\mathbf{\Pi}_v)\right\} = \lambda_u\,|\mathcal{A}|\,p \tag{2}$$

where

$$p = \mathbb{E}_{\mathbf{\Pi}_v}\{g(\boldsymbol{\omega},\mathbf{\Pi}_v)\}\ . \tag{3}$$

[2]For example, r_l corresponds to the maximum distance that makes an average SNR not less than a minimum required value, depending on the receiver sensitivity and communication reliability.

[3]The probabilistic behavior of $\mathbf{G}(\mathbf{x})$ depends on $\mathbf{\Pi}_{\ell}^{(l-1)}$ process according to the PAR.

[4]Our framework is valid for various MAC protocols. An example of MAC protocol will be presented in Sec. V.

Proof: The left side of (1) can be written as

$$\begin{aligned}
&\mathbb{E}_{\mathbf{\Pi}_u,\mathbf{\Pi}_v}\left\{\sum_{\mathbf{X}\in\mathbf{\Pi}_u\cap\mathcal{A}} g(\mathbf{X},\mathbf{\Pi}_v)\right\} \qquad (4)\\
&\quad= \mathbb{E}_{\mathbf{\Pi}_v}\left\{\mathbb{E}_{\mathbf{\Pi}_u}\left\{\sum_{\mathbf{X}\in\mathbf{\Pi}_u} \mathbb{1}_{\mathcal{A}}(\mathbf{X})\, g(\mathbf{X},\mathbf{\Pi}_v)\right\}\right\}\\
&\quad\overset{(a)}{=} \mathbb{E}_{\mathbf{\Pi}_v}\left\{\int_{\mathcal{A}} g(\boldsymbol{\omega},\mathbf{\Pi}_v)\,\mu_u(d\boldsymbol{\omega})\right\}\\
&\quad\overset{(b)}{=} \lambda_u\,\mathbb{E}_{\mathbf{\Pi}_v}\left\{\int_{\mathcal{A}} g(\boldsymbol{\omega},\mathbf{\Pi}_v)\right\} d\boldsymbol{\omega}\\
&\quad\overset{(c)}{=} \lambda_u \int_{\mathcal{A}} \mathbb{E}_{\mathbf{\Pi}_v}\{g(\boldsymbol{\omega},\mathbf{\Pi}_v)\}\, d\boldsymbol{\omega}
\end{aligned}$$

where $\mu_u(d\boldsymbol{\omega})$ is the average number of nodes in $d\boldsymbol{\omega}$ and

$$\mathbb{1}_{\mathcal{A}}(\boldsymbol{\omega}) \triangleq \begin{cases} 1, & \text{if } \boldsymbol{\omega} \in \mathcal{A} \\ 0, & \text{otherwise}\,. \end{cases} \tag{5}$$

In (4), (a) is from the Campbell's theorem [53], (b) holds for a homogeneous PPP, and (c) is true for finite $\mathbb{E}_{\mathbf{\Pi}_v}\{\int_{\mathcal{A}} |g(\boldsymbol{\omega},\mathbf{\Pi}_v)|\, d\boldsymbol{\omega}\}$. When the process $g(\boldsymbol{\omega},\mathbf{\Pi}_v)$ is stationary, we have

$$\lambda_u \int_{\mathcal{A}} \mathbb{E}_{\mathbf{\Pi}_v}\{g(\boldsymbol{\omega},\mathbf{\Pi}_v)\}\, d\boldsymbol{\omega} = \lambda_u\,|\mathcal{A}|\,p$$

where p is given by (3). □

We now obtain the spatial density of nodes in a cluster according to the aforementioned PAR.

Lemma 2 (Node density in a typical cluster): The spatial density of nodes in a typical lth-level cluster is

$$\lambda_{\mathrm{c}}^{(l)} = p_{\mathrm{ga}}^{(l)} \lambda_{\ell}^{(l)} \tag{6}$$

where $p_{\mathrm{ga}}^{(l)}$ is the probability of gateway association given by

$$p_{\mathrm{ga}}^{(l)} = \frac{1 - \exp\left\{-\lambda_{\ell}^{(l-1)} B(r_l)\right\}}{\lambda_{\ell}^{(l-1)} B(r_l)}\ . \tag{7}$$

Proof: The average number of nodes at level l associated with a typical GN at the origin $\mathbf{o}$ is given by

$$\mathbb{E}_{\mathbf{\Pi}_\ell^{(l)},\,\mathbf{\Pi}_\ell^{(l-1)}}\left\{\sum_{\mathbf{X}\in\mathbf{\Pi}_\ell^{(l)}\cap\mathcal{B}_\mathbf{o}(r_l)}\mathbb{1}_{\mathcal{P}_{l-1}(\mathbf{o})}(\mathbf{X})\right\} \tag{8}$$

where $\mathcal{P}_{l-1}(\mathbf{y}) = \{\mathbf{x}\in\mathcal{B}_\mathbf{y}(r_l) : \mathbf{G}(\mathbf{x}) = \mathbf{y}\}$ is the *random set* of all potential positions where nodes in level l associate with the GN in level $l-1$ at $\mathbf{y}$. The probabilistic behavior of $\mathcal{P}_{l-1}(\mathbf{y})$ depends on $\mathbf{\Pi}_\ell^{(l-1)}$. Using Lemma 1 with $\mathbf{\Pi}_u = \mathbf{\Pi}_\ell^{(l)}$, $\mathbf{\Pi}_v = \mathbf{\Pi}_\ell^{(l-1)}$, $\lambda_u = \lambda_\ell^{(l)}$, and $\mathcal{A} = \mathcal{B}_\mathbf{o}(r_l)$, we have

$$\mathbb{E}_{\mathbf{\Pi}_\ell^{(l)},\,\mathbf{\Pi}_\ell^{(l-1)}}\left\{\sum_{\mathbf{X}\in\mathbf{\Pi}_\ell^{(l)}\cap\mathcal{B}_\mathbf{o}(r_l)}\mathbb{1}_{\mathcal{P}_{l-1}(\mathbf{o})}(\mathbf{X})\right\} = \lambda_\ell^{(l)}B(r_l)\,p_{\text{ga}}^{(l)} \tag{9}$$

where

$$p_{\text{ga}}^{(l)} = \mathbb{P}\left\{\mathbf{x}\in\mathcal{P}_{l-1}(\mathbf{o})\right\} \qquad \mathbf{x}\in\mathcal{B}_\mathbf{o}(r_l) \tag{10}$$

is the probability that a node in level l, within the radius r_l from the typical GN, associates with the typical GN. Using the total probability theorem, (10) becomes

$$p_{\text{ga}}^{(l)} = \sum_{n=0}^{\infty}\frac{1}{n+1}\frac{\left(\lambda_\ell^{(l-1)}B(r_l)\right)^n}{n!}\exp\left\{-\lambda_\ell^{(l-1)}B(r_l)\right\} \tag{11}$$

which results in (7). Dividing (9) by $B(r_l)$ gives the spatial density of nodes in a typical lth-level cluster as (6). □

B. Signal-to-Noise Ratio Characterization

The instantaneous SNR per symbol received by a node at $\mathbf{Y}\in\mathbf{\Pi}_v$ from a node in level l at $\mathbf{x}$ is given by[5]

$$\zeta_v^{(l)} = \frac{E_{\text{b}}^{(l)}R_\ell\,G_0\,|H_{\mathbf{x},\mathbf{Y}}|^2}{N_0W}D_{\mathbf{x},\mathbf{Y}}^{-\alpha} \tag{12}$$

where $E_{\text{b}}^{(l)}$ is the average transmitted energy per bit from a node at level l; N_0 is the one-sided power spectral density (PSD) of the additive white Gaussian noise (AWGN); R_ℓ is the data rate ($R_\ell T$ bits transmitted in a symbol duration T); W is the transmission bandwidth; G_0 is a constant that depends on the antenna gains and the wavelength; $D_{\mathbf{x},\mathbf{Y}} = \|\mathbf{x}-\mathbf{Y}\|$ is the distance between the transmitter and receiver; $H_{\mathbf{x},\mathbf{Y}}$ is the fading level of the link; and α is the pathloss exponent.

We now determine the complementary cumulative distribution function (CCDF) of the received SNR.

Lemma 3 (CCDF of the received SNR in generic fading): The CCDF of the SNR received by a node at $\mathbf{Y}\in\mathbf{\Pi}_v$ from a node in level l at $\mathbf{x}$ is given by

$$\overline{F}_{\zeta_v^{(l)}}(\xi) = \frac{1}{2} + \int_0^\infty \frac{\mathfrak{Im}\left\{\phi_{|H_{\mathbf{x},\mathbf{Y}}|^2}(\jmath\omega)\,\phi_{D_{\mathbf{x},\mathbf{Y}}^\alpha}\left(-\jmath\omega\frac{\xi N_0W}{E_{\text{b}}^{(l)}R_\ell G_0}\right)\right\}}{\pi\omega}d\omega \tag{13}$$

where $\phi_V(\jmath\omega)$ is the characteristic function (CF) of the random variable V. The CF of $D_{\mathbf{x},\mathbf{Y}}^\alpha$ is given by

$$\phi_{D_{\mathbf{x},\mathbf{Y}}^\alpha}(\jmath\omega) = \frac{2\,(-\jmath\omega)^{-2/\alpha}}{\alpha r_l^2}\,\gamma\left(\frac{2}{\alpha},-\jmath\omega\,r_l^\alpha\right) \tag{14}$$

where $\gamma(\cdot,\cdot)$ is the lower incomplete Gamma function [54].

Proof: The CCDF of the received SNR in (12) conditioned on D, is equal to[6]

$$\mathbb{P}\left\{\zeta_v^{(l)} > \xi \mid D\right\} = \overline{F}_U(0)$$

where $U = |H|^2 - \frac{N_0W}{E_{\text{b}}^{(l)}R_\ell G_0}D^\alpha\xi$. The CF of U is given by

$$\phi_U(\jmath\omega) = \phi_{|H|^2}(\jmath\omega)\,e^{-\jmath\omega\frac{\xi N_0WD^\alpha}{E_{\text{b}}^{(l)}R_\ell G_0}}.$$

By using the inversion theorem,[7] the conditional CCDF of the received SNR results in

$$\overline{F}_{\zeta_v^{(l)}|D}(\xi) = \frac{1}{2} + \int_0^\infty \frac{\mathfrak{Im}\left\{e^{-\jmath\omega\frac{\xi N_0WD^\alpha}{E_{\text{b}}^{(l)}R_\ell G_0}}\phi_{|H|^2}(\jmath\omega)\right\}}{\pi\,\omega}d\omega. \tag{15}$$

It can be shown that D^2 follows a uniform distribution in the interval $\left(0, r_l^2\right]$. Therefore, for a random distance D, the CCDF in (15) is now given by (13) where

$$\phi_{D^\alpha}(\jmath\omega) = \frac{2}{r_l^2}\int_0^{r_l}\xi e^{\jmath\omega\xi^\alpha}d\xi$$

which results in (14). □

C. Multilevel Network Lifetime

Nodes in the network drain the battery energy due to multiple modes of operations such as transmitting, receiving, listening, and processing [56]. Compared to other modes, transmitting mode usually dominates the energy consumption and thus the node's lifetime. We now determine the average energy consumption per node per round and the network lifetime based on the energy consumption of all transmitting nodes.[8] In each round, every node generates b_{g} bits to communicate the observed physical quantity. A node in level L communicates b_{g} bits to its GN and a node in level $l = L-1, L-2, \cdots, 1$ communicates its own b_{g} bits together with those successfully collected from nodes in level $l+1$. The total number of bits communicated by a node in level l at $\mathbf{x}$ is then mapped into $s_l(\mathbf{x})$ symbols according to the signaling constellation.

Lemma 4 (Average energy consumption): The average energy consumption per node in a round is given by

$$E_{\text{round}} = E_{\text{b}}^{(L)}R_\ell T\sum_{l=1}^{L}\Delta_l\,s_l\,\beta^{(l)}\,p_{\text{t}}^{(l)} \tag{16}$$

[5]For a legitimate receiver $\mathbf{\Pi}_v = \mathbf{\Pi}_\ell^{(l-1)}$ and for an eavesdropper $\mathbf{\Pi}_v = \mathbf{\Pi}_{\text{e}}^{(l)}$. For notational brevity, we suppress the dependence of $\zeta_v^{(l)}$ on $\mathbf{x}$ and $\mathbf{Y}$.

[6]For simplicity, we use D and $|H|^2$ instead of $D_{\mathbf{x},\mathbf{Y}}$ and $|H_{\mathbf{x},\mathbf{Y}}|^2$.

[7]For a random variable X, the inversion theorem provides [55]

$$\overline{F}_U(u) = \frac{1}{2} + \frac{1}{\pi}\int_0^\infty\frac{\mathfrak{Im}\left\{e^{-\jmath\omega u}\phi_u(\jmath\omega)\right\}}{\omega}d\omega.$$

[8]Note that energy consumption of other modes can be included in the evaluation of the nodes' lifetime (see e.g., [5], [57]).

where, in a level l, Δ_l is the transmission energy ratio so that $E_{\mathrm{b}}^{(l)} = \Delta_l E_{\mathrm{b}}^{(L)}$, s_l is the average number of symbols transmitted by a node per round, given by

$$s_l = \mathbb{E}_{\cup_{k=l+1}^{L} \mathbf{\Pi}_\ell^{(k)}} \{ s_l(\mathbf{x}) \} \tag{17}$$

and $p_{\mathrm{t}}^{(l)}$ is the transmission probability of a node, given by

$$p_{\mathrm{t}}^{(l)} = 1 - \exp\left\{ -\lambda_\ell^{(l-1)} B\left(r_l\right) \right\}. \tag{18}$$

Proof: Consider legitimate nodes of an MWN in a bounded space $\mathcal{A} \subset \mathbb{R}^d$, which is a Borel set of $\mathbb{R}^d$ with volume $|\mathcal{A}| \gg B(r_l)$ for all l. The average energy consumption per node per round is given by

$$\begin{aligned} & E_{\text{round}} \\ &= \frac{R_\ell T}{\lambda_\ell |\mathcal{A}|} \mathbb{E}_{\mathbf{\Pi}_\ell} \left\{ \sum_{l=1}^{L} \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \mathbb{1}_{\mathcal{T}_{l-1}}(\mathbf{X})\, s_l(\mathbf{X})\, E_{\mathrm{b}}^{(l)} \right\} \\ &= \frac{R_\ell T}{\lambda_\ell |\mathcal{A}|} \sum_{l=1}^{L} \mathbb{E}_{\cup_{k=l-1}^{L} \mathbf{\Pi}_\ell^{(k)}} \left\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \mathbb{1}_{\mathcal{T}_{l-1}}(\mathbf{X})\, s_l(\mathbf{X})\, E_{\mathrm{b}}^{(l)} \right\} \end{aligned} \tag{19}$$

where

$$\mathcal{T}_{l-1} = \left\{ \mathbf{x} \in \mathbb{R}^d : |\mathcal{G}_{l-1}(\mathbf{x})| \neq 0 \right\} \tag{20}$$

is the random set of all positions, where nodes in level l transmit to GNs in level $l-1$. Since $\mathcal{T}_{l-1}$ depends only on $\mathbf{\Pi}_\ell^{(l-1)}$ and $s_l(\mathbf{x})$ depends only on $\mathbf{\Pi}_\ell^{(l+1)}, \mathbf{\Pi}_\ell^{(l+2)} \ldots, \mathbf{\Pi}_\ell^{(L)}$, we can rewrite (19) as

$$E_{\text{round}} = \frac{E_{\mathrm{b}}^{(L)} R_\ell T}{\lambda_\ell |\mathcal{A}|} \sum_{l=1}^{L} \Delta_l s_l \mathbb{E}_{\mathbf{\Pi}_\ell^{(l)}, \mathbf{\Pi}_\ell^{(l-1)}} \left\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \mathbb{1}_{\mathcal{T}_{l-1}}(\mathbf{X}) \right\} \tag{21}$$

where s_l is given by (17). Using Lemma 1 with $\mathbf{\Pi}_u = \mathbf{\Pi}_\ell^{(l)}$, $\mathbf{\Pi}_v = \mathbf{\Pi}_\ell^{(l-1)}$, $\lambda_u = \lambda_\ell^{(l)}$, we have

$$\mathbb{E}_{\mathbf{\Pi}_\ell^{(l)}, \mathbf{\Pi}_\ell^{(l-1)}} \left\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \mathbb{1}_{\mathcal{T}_{l-1}}(\mathbf{X}) \right\} = \lambda_\ell |\mathcal{A}|\, \beta^{(l)}\, p_{\mathrm{t}}^{(l)} \tag{22}$$

where

$$p_{\mathrm{t}}^{(l)} = \mathbb{P}\left\{ \mathbf{x} \in \mathcal{T}_{l-1} \right\}$$

is the probability that a node in level l has a GN in level $l-1$, which results in (18). By substituting (22) into (21), we obtain (16). □

The network lifetime is defined as the average number of rounds, N_{round}, that a node can operate during its life. It is given by

$$N_{\text{round}} = \frac{E_{\text{charged}}}{E_{\text{round}}} \tag{23}$$

where E_{charged} is the fully-charged energy of node battery. Using Lemma 4, N_{round} becomes

$$N_{\text{round}} = \frac{E_{\text{charged}}}{E_{\mathrm{b}}^{(L)} R_\ell T \sum_{l=1}^{L} \Delta_l\, s_l\, \beta^{(l)}\, p_{\mathrm{t}}^{(l)}}. \tag{24}$$

III. Distributed Network Secrecy Concept

The secrecy of a self-organizing MWN is affected by the spatial distribution of nodes, the type of communication protocols, the quality of all legitimate links, and the capability of eavesdropping networks. We now define a new metric for MWNs based on inter-level network secrecy and DNS.

Definition 1 (Inter-level network secrecy): The inter-level communication from a node in level k at $\mathbf{x}$ to its GN in level $k-1$ achieves network secrecy when the following event $\mathcal{S}_{\mathbf{x}}^{(k)}$ is true

$$\mathcal{S}_{\mathbf{x}}^{(k)} = \mathcal{T}_{\mathbf{x}}^{(k)} \wedge \overline{\mathcal{C}}_{\mathbf{x}}^{(k)} \wedge \mathcal{R}_{\mathbf{x}}^{(k)} \wedge \overline{\mathcal{E}}_{\mathbf{x}}^{(k)} \tag{25}$$

where the events $\mathcal{T}_{\mathbf{x}}^{(k)}$, $\mathcal{C}_{\mathbf{x}}^{(k)}$, $\mathcal{R}_{\mathbf{x}}^{(k)}$, and $\mathcal{E}_{\mathbf{x}}^{(k)}$ are defined in the following.

1) *Transmission event* $\mathcal{T}_{\mathbf{x}}^{(k)}$: this event occurs when a legitimate transmitter in level k at $\mathbf{x}$ has a GN in level $k-1$, i.e., $\mathbf{x} \in \mathcal{T}_{k-1}$ where $\mathcal{T}_{k-1}$ is given by (20).

2) *Collision event* $\mathcal{C}_{\mathbf{x}}^{(k)}$: this event occurs when a legitimate node in level k at $\mathbf{x}$ transmits using the communication resources that are also used by other legitimate nodes in a bounded space $\mathcal{A}$, i.e., $\mathbf{x} \in \mathcal{C}_k$ where

$$\mathcal{C}_k = \left\{ \mathbf{x} \in \mathbb{R}^d : |\mathcal{Z}_k(\mathbf{x})| \neq 0 \right\} \tag{26}$$

with $\mathcal{Z}_k(\mathbf{x})$ denoting the random set of all other nodes in level k using the same resources as the node at $\mathbf{x}$.

3) *Successful reception event* $\mathcal{R}_{\mathbf{x}}^{(k)}$: this event occurs when the SNR $\zeta_\ell^{(k)}$ received by the GN in level $k-1$ from its associated legitimate transmitter in level k at $\mathbf{x}$ is greater than a threshold value $\check{\zeta}_\ell$,[9] i.e., $\mathbf{x} \in \mathcal{R}_{k-1}$ where

$$\mathcal{R}_{k-1} = \left\{ \mathbf{x} \in \mathbb{R}^d : \zeta_\ell^{(k)} > \check{\zeta}_\ell \right\}. \tag{27}$$

4) *Eavesdropping event* $\mathcal{E}_{\mathbf{x}}^{(k)}$: this event occurs when the SNR $\zeta_{\mathrm{e}}^{(k)}$ received by at least one eavesdropping node, from a legitimate transmitter in level k at $\mathbf{x}$, is greater than a threshold value $\check{\zeta}_{\mathrm{e}}$, i.e., $\mathbf{x} \in \mathcal{E}_k$ where

$$\mathcal{E}_k = \left\{ \mathbf{x} \in \mathbb{R}^d : \max_{\mathbf{x}_{\mathrm{e}} \in \mathbf{\Pi}_{\mathrm{e}}^{(k)}} \zeta_{\mathrm{e}}^{(k)} > \check{\zeta}_{\mathrm{e}} \right\}. \tag{28}$$

We consider that legitimate transmitters do not have channel knowledge for legitimate and eavesdropping links. The SNR threshold values $\check{\zeta}_\ell$ and $\check{\zeta}_{\mathrm{e}}$ are set to provide secrecy rate R_{s} when the event in (25) is true, where

$$R_{\mathrm{s}} = [R_\ell - W \log_2\left(1 + \check{\zeta}_{\mathrm{e}}\right)]^+ \tag{29}$$

and $R_\ell \leq W \log_2\left(1 + \check{\zeta}_\ell\right)$. Since $R_{\mathrm{s}} \leq R_\ell$, the fraction R_{s}/R_ℓ bits can be transmitted confidentially, translating to $b_{\mathrm{s}} \in [0, b_{\mathrm{g}}]$ transmitted confidential bits per node per round [cbits/node/round].

The DNS is achieved when inter-level network secrecy is obtained in all levels, that is, data transmitted without collision are received successfully without being successfully eavesdropped in all levels. With this observation, we define DNS in the following.

[9]The required SNR depends on employed signaling constellation and diversity method [58].

Definition 2 (Distributed network secrecy): For a node in level l at $\mathbf{x}$ communicating to a monitor, the DNS is achieved when the event

$$\wedge_{k=1}^{l} \mathcal{S}_{\mathbf{x}}^{(k)} \tag{30}$$

is true, where $\mathcal{S}_{\mathbf{x}}^{(k)}$ is defined in (25). When $l = L$ full DNS is achieved.

Remark 2: Data from a node in level l are transmitted l times over different inter-level communication resources to reach the monitor. This multi-hop transmission may give malicious nodes multiple opportunities for eavesdropping. On the other hand, multi-hop transmission may reduce the amount of energy required to communicate with the monitor. Therefore, the operating parameters (e.g., nodes density and transmitted energy) in each level of the self-organized MWN determine the relationship between the DNS and the network lifetime.

We now define a metric to characterize the DNS in an MWN.

Definition 3 (DNS throughput): In an MWN with L levels, the DNS throughput is defined as

$$\rho_{\text{ds}} \triangleq \frac{b_{\text{s}}}{\lambda_\ell \left|\mathcal{A}\right|} \mathbb{E}_{\mathbf{\Pi}_\ell, \mathbf{\Pi}_{\text{e}}} \left\{ \sum_{l=1}^{L} \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \prod_{k=1}^{l} \mathbb{1}_{\mathcal{S}_k}\Big(\varphi_k^{(l)}(\mathbf{X})\Big) \right\} \tag{31}$$

where[10]

$$\varphi_k^{(l)}(\mathbf{x}) = \begin{cases} \mathbf{x}, & \text{for } k = l \\ (\mathbf{G} \circ \varphi_{k+1}^{(l)})(\mathbf{x}), & \text{for } k = l-1, l-2, \cdots, 1 \end{cases}$$

is the node in level l at $\mathbf{x}$ for $k = l$ and its GN at level k for $k < l$, and

$$\mathcal{S}_k = \mathcal{T}_{k-1} \cap \overline{\mathcal{C}}_k \cap \mathcal{R}_{k-1} \cap \overline{\mathcal{E}}_k$$

is the random set of all positions from which nodes in level k transmit without collision, with successful reception, and without being successfully eavesdropped.

Remark 3: The product of indicator functions in (31) accounts for secure transmission of b_{s} bits from level l to level 1 in a round. Therefore, the DNS throughput measures the average number of bits that a node communicates with DNS in a round, and its unit is cbits/node/round. One can also define variants of the DNS throughput starting from ρ_{ds} in (31), for example, $\lambda_\ell \rho_{\text{ds}}$ denotes the throughput in cbits/m^2/round.

Example 1: In the case of a two-level network, (31) with $L = 2$ becomes

$$\rho_{\text{ds}} = \frac{b_{\text{s}}}{\lambda_\ell \left|\mathcal{A}\right|} \mathbb{E}_{\mathbf{\Pi}_\ell, \mathbf{\Pi}_{\text{e}}} \left\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(1)} \cap \mathcal{A}} \mathbb{1}_{\mathcal{S}_1}(\mathbf{X}) + \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(2)} \cap \mathcal{A}} \mathbb{1}_{\mathcal{S}_2}(\mathbf{X})\, \mathbb{1}_{\mathcal{S}_1}(\mathbf{G}(\mathbf{X})) \right\}. \tag{32}$$

[10]Notation $(f \circ g)(x)$ stands for composition $f(g(x))$.

IV. Distributed Network Secrecy Analysis

In this section, we first analyze the DNS throughput for various network configurations in generic fading channels, and then derive its closed-form expressions in Nakagami-m fading channels.

A. Generic Fading Channels

Theorem 1 (DNS throughput in generic fading): The DNS throughput of an MWN with L levels is given by

$$\rho_{\text{ds}} = b_{\text{s}} \sum_{l=1}^{L} \beta^{(l)} \prod_{k=1}^{l} p_{\text{t}}^{(k)} p_{\bar{\text{c}}}^{(k)} p_{\text{r}}^{(k)} p_{\bar{\text{e}}}^{(k)} \tag{33}$$

with

$$p_{\text{t}}^{(k)} = 1 - \exp\left\{-\lambda_\ell^{(k-1)} B\left(r_k\right)\right\} \tag{34}$$

$$p_{\bar{\text{c}}}^{(k)} = \mathbb{E}_{\mathbf{\Pi}_\ell^{(k)}}\left\{ \mathbb{1}_{\overline{\mathcal{C}}_k}\Big(\varphi_k^{(l)}(\mathbf{x})\Big) \right\} \tag{35}$$

$$p_{\text{r}}^{(k)} = \overline{F}_{\zeta_\ell^{(k)}}\left(\check{\zeta}_\ell\right) \tag{36}$$

$$p_{\bar{\text{e}}}^{(k)} = \exp\left\{-\lambda_{\text{e}}^{(k)} \int_{\mathbb{R}^d} \overline{F}_{\zeta_{\text{e}}^{(k)} | d_{\mathbf{x},\boldsymbol{\omega}}}\left(\check{\zeta}_{\text{e}}\right) d\boldsymbol{\omega}\right\} \tag{37}$$

where, for a transmitter in level k, $p_{\text{t}}^{(k)}$ is the transmission probability, $p_{\bar{\text{c}}}^{(k)}$ is the probability of no collision, $p_{\text{r}}^{(k)}$ is the probability of successful reception, and $p_{\bar{\text{e}}}^{(k)}$ is the probability of unsuccesful eavesdropping.

Proof: For a transmitter in level k, the random sets $\mathcal{T}_{k-1}$ and $\mathcal{R}_{k-1}$ depend on $\mathbf{\Pi}_\ell^{(k-1)}$, $\mathcal{C}_k$ depends on $\mathbf{\Pi}_\ell^{(k)}$, and $\mathcal{E}_k$ depends on $\mathbf{\Pi}_{\text{e}}^{(k)}$. Therefore,

$$\mathbb{E}_{\mathbf{\Pi}_\ell, \mathbf{\Pi}_{\text{e}}}\left\{ \sum_{l=1}^{L} \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \prod_{k=1}^{l} \mathbb{1}_{\mathcal{S}_k}\Big(\varphi_k^{(l)}(\mathbf{X})\Big) \right\} \tag{38}$$

$$= \sum_{l=1}^{L} \mathbb{E}_{\mathbf{\Pi}_\ell^{(l)}}\Bigg\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \mathbb{1}_{\overline{\mathcal{C}}_l}\Big(\varphi_l^{(l)}(\mathbf{X})\Big) \times \mathbb{E}_{\bigcup_{k=1}^{l-1} \mathbf{\Pi}_\ell^{(k)}, \mathbf{\Pi}_{\text{e}}}\Bigg\{ \prod_{k=1}^{l-1} \mathbb{1}_{\overline{\mathcal{C}}_k}\Big(\varphi_k^{(l)}(\mathbf{X})\Big) \times \prod_{k=1}^{l} \mathbb{1}_{\mathcal{T}_{k-1}}\Big(\varphi_k^{(l)}(\mathbf{X})\Big)\, \mathbb{1}_{\mathcal{R}_{k-1}}\Big(\varphi_k^{(l)}(\mathbf{X})\Big)\, \mathbb{1}_{\overline{\mathcal{E}}_k}\Big(\varphi_k^{(l)}(\mathbf{X})\Big) \Bigg\} \Bigg\}.$$

Note that $\mathcal{T}_{k-1}$ depends on the *presence* of at least one node in level $k-1$ within a distance r_k from $\varphi_k^{(l)}(\mathbf{x})$, $\mathcal{R}_{k-1}$ depends on the *distance* between $\varphi_k^{(l)}(\mathbf{x})$ and $\varphi_{k-1}^{(l)}(\mathbf{x})$, and $\mathcal{C}_{k-1}$ depends on the *number* of level $k-1$ nodes, each transmitting to its associated GN according to a communication protocol. Therefore, the right side of (38) can be written as[11]

$$\sum_{l=1}^{L} \mathbb{E}_{\mathbf{\Pi}_\ell^{(l)}}\Bigg\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_\ell^{(l)} \cap \mathcal{A}} \mathbb{1}_{\overline{\mathcal{C}}_l}\Big(\varphi_l^{(l)}(\mathbf{X})\Big) \Bigg\} \times \prod_{k=1}^{l} p_{\text{t}}^{(k)} p_{\text{r}}^{(k)} p_{\bar{\text{e}}}^{(k)} \prod_{k=1}^{l-1} p_{\bar{\text{c}}}^{(k)}. \tag{39}$$

[11]For the case where all eavesdropping nodes aim to intercept legitimate transmissions at each level, care must be taken to evaluate the expectation of $\prod_{k=1}^{l} \mathbb{1}_{\overline{\mathcal{E}}_k}\Big(\varphi_k^{(l)}(\mathbf{X})\Big)$.

$$\rho_{\mathrm{ds}} = b_{\mathrm{s}} \sum_{l=1}^{L} \beta^{(l)} \left\{ \prod_{k=1}^{l} p_{\mathrm{c}}^{(k)} \left[1 - e^{-\lambda_{\ell}^{(k-1)} \pi r_k^2} \right] \left(\frac{E_{\mathrm{b}}^{(k)} R_{\ell} G_0}{\check{\zeta}_{\ell} N_0 W} \right)^{2/\alpha} \frac{2}{\alpha r_k^2} \sum_{t=0}^{m-1} \frac{1}{t!} \gamma \left(\frac{2}{\alpha} + t, \frac{\check{\zeta}_{\ell} N_0 W r_k^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right) \right.$$
$$\left. \times \exp \left\{ -\frac{2\pi \lambda_{\mathrm{e}}^{(k)}}{\alpha} \left(\frac{E_{\mathrm{b}}^{(k)} R_{\ell} G_0}{\check{\zeta}_{\mathrm{e}} N_0 W} \right)^{2/\alpha} \sum_{t=0}^{m-1} \frac{1}{t!} \Gamma \left(\frac{2}{\alpha} + t \right) \right\} \right\} \quad (42)$$

The $p_{\bar{\mathrm{c}}}^{(k)}$ is the probability that a node in level k transmits without collision and can be written as (35).[12] The $p_{\mathrm{t}}^{(k)}$ is the probability that a node in level k transmits to a GN and can be written as (18). The $p_{\mathrm{r}}^{(k)}$ is the probability that a GN in level $k-1$ successfully receives data transmitted by a node in level k, and can be written as $p_{\mathrm{r}}^{(k)} = \mathbb{P}\{\mathbf{x} \in \mathcal{R}_{k-1}\}$. From (27), we have

$$p_{\mathrm{r}}^{(k)} = \mathbb{E}_{D_{\mathbf{x},\mathbf{G}(\mathbf{x})}} \left\{ \overline{F}_{\zeta_{\ell}^{(k)} | D_{\mathbf{x},\mathbf{G}(\mathbf{x})}} \left(\check{\zeta}_{\ell} \right) \right\}$$

which results in (36). Finally, $p_{\bar{\mathrm{e}}}^{(k)}$ is the probability that a node in level k transmits without being successfully eavesdropped and can be written as $p_{\bar{\mathrm{e}}}^{(k)} = \mathbb{P}\left\{\mathbf{x} \in \overline{\mathcal{E}}_k\right\}$. From (28) and the stationarity of $\mathbf{\Pi}_{\mathrm{e}}$, we have

$$p_{\bar{\mathrm{e}}}^{(k)} = \mathbb{E}_{\mathbf{\Pi}_{\mathrm{e}}^{(k)}} \left\{ \mathbb{P} \left\{ \max_{\mathbf{X}_{\mathrm{e}} \in \mathbf{\Pi}_{\mathrm{e}}^{(k)}} \zeta_{\ell | D_{\mathbf{x},\mathbf{X}_{\mathrm{e}}}}^{(k)} \leq \check{\zeta}_{\mathrm{e}} \right\} \right\}$$
$$= \mathbb{E}_{\mathbf{\Pi}_{\mathrm{e}}^{(k)}} \left\{ \prod_{\mathbf{X}_{\mathrm{e}} \in \mathbf{\Pi}_{\mathrm{e}}^{(k)}} \left[1 - \overline{F}_{\zeta_{\ell | D_{\mathbf{x},\mathbf{X}_{\mathrm{e}}}}^{(k)}} \left(\check{\zeta}_{\mathrm{e}} \right) \right] \right\}. \quad (40)$$

By using the probability generating functional of a PPP, we obtain (37).[13] Recall that the collision event of a node in level k at $\mathbf{x}$ depends on the communication resources utilized by the other nodes in level k. It follows that the random set $\mathcal{C}_k$ depends on the process $\mathbf{\Pi}_{\ell}^{(k)} \backslash \{\mathbf{x}\}$. Therefore, by using the reduced Campbell formula [59], we can write the expectation in (39) as

$$\mathbb{E}_{\mathbf{\Pi}_{\ell}^{(l)}} \left\{ \sum_{\mathbf{X} \in \mathbf{\Pi}_{\ell}^{(l)} \cap \mathcal{A}} \mathbb{1}_{\overline{\mathcal{C}}_l} \left(\varphi_l^{(l)}(\mathbf{X}) \right) \right\}$$
$$= \lambda_{\ell}^{(l)} \int_{\mathcal{A}} \mathbb{E}_{\mathbf{\Pi}_{\ell}^{(l)}} \left\{ \mathbb{1}_{\overline{\mathcal{C}}_l} \left(\varphi_l^{(l)}(\boldsymbol{\omega}) \right) \right\} d\boldsymbol{\omega}$$
$$= \lambda_{\ell}^{(l)} p_{\bar{\mathrm{c}}}^{(l)} |\mathcal{A}| . \quad (41)$$

Therefore, by substituting (41) into (39) and using (31), the DNS throughput results in (33). □

Remark 4: Theorem 1 enables the evaluation of the DNS throughput for MWNs as a function of the CCDF of received SNRs, node spatial distribution, multilevel cluster formation, propagation medium, and communication protocol.

[12]Closed form expressions can be obtained depending on the communication protocol.

[13]Let $\nu(\mathbf{x})$ be a bounded measurable function of $\mathbf{x} \in \mathbb{R}^d$. The generating functional of a point process $\mathbf{\Pi}$ is $G(\nu) = \mathbb{E}_{\mathbf{\Pi}}\{\prod_{\mathbf{X} \in \mathbf{\Pi}} \nu(\mathbf{X})\}$. By Campbell's theorem [53], it is equal to

$$G(\nu) = \exp \left\{ -\int_{\mathbb{R}^d} (1 - \nu(\mathbf{x})) \, \Lambda(d\mathbf{x}) \right\}$$

for a PPP with the spatial density $\Lambda(\mathbf{x})$.

B. Nakagami-m Fading Channels

We now derive the closed-form expression for the DNS throughput in Nakagami-m fading channels.

Theorem 2 (DNS throughput for Nakagami-m fading): The DNS throughput in Nakagami-m fading channels is given by (42), shown at the top of this page, for positive integer m.

Proof: The DNS throughput is obtained from Theorem 1 by determining the CCDF of the SNR in (36) and (37) for Nakagami-m fading channels. Using (12), the CCDF of the SNR received by a node at $\mathbf{Y} \in \mathbf{\Pi}_v$ conditioned on the distance D from a transmitter in level k at $\mathbf{x}$ is

$$\overline{F}_{\zeta_{v|D}^{(k)}}(\xi) = \overline{F}_{|H|^2} \left(\frac{\xi N_0 W D^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right).$$

Therefore,

$$\overline{F}_{\zeta_{v|D}^{(k)}}(\xi) = \sum_{t=0}^{m-1} \frac{1}{t!} \left(\frac{\xi N_0 W D^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right)^{t} \exp \left\{ -\frac{\xi N_0 W D^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right\} \quad (43)$$

for Nakagami-m fading channels [60]. Since the squared distances are uniformly distributed between 0 and r_k^2, the CCDF of the received SNR averaged over the distance distribution results in

$$p_{\mathrm{r}}^{(k)} = \frac{2}{r_k^2} \sum_{t=0}^{m-1} \frac{1}{t!} \left(\frac{\xi N_0 W}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right)^{t} \quad (44)$$
$$\times \int_0^{r_k} y^{\alpha t + 1} \exp \left\{ -\frac{\xi N_0 W y^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right\} dy$$
$$= \frac{2}{\alpha r_k^2} \left(\frac{E_{\mathrm{b}}^{(k)} R_{\ell} G_0}{\xi N_0 W} \right)^{2/\alpha} \sum_{t=0}^{m-1} \frac{1}{t!} \gamma \left(\frac{2}{\alpha} + t, \frac{\xi N_0 W r_k^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right).$$

For the eavesdropping network, substituting (43) into (37), the probability of unsuccessful eavesdropping in level $k = L, L-1, \cdots, 1$ becomes

$$p_{\bar{\mathrm{e}}}^{(k)} = \exp \left\{ -2\pi \lambda_{\mathrm{e}}^{(k)} \sum_{t=0}^{m-1} \frac{1}{t!} \left(\frac{\check{\zeta}_{\mathrm{e}} N_0 W}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right)^{t} \right.$$
$$\left. \times \int_0^{\infty} y^{1+\alpha t} \exp \left\{ -\frac{\check{\zeta}_{\mathrm{e}} N_0 W y^{\alpha}}{E_{\mathrm{b}}^{(k)} R_{\ell} G_0} \right\} dy \right\}$$
$$= \exp \left\{ -\frac{2\pi \lambda_{\mathrm{e}}^{(k)}}{\alpha} \left(\frac{E_{\mathrm{b}}^{(k)} R_{\ell} G_0}{\check{\zeta}_{\mathrm{e}} N_0 W} \right)^{2/\alpha} \sum_{t=0}^{m-1} \frac{1}{t!} \Gamma \left(\frac{2}{\alpha} + t \right) \right\} \quad (45)$$

where $\Gamma(\cdot)$ is the Gamma function [54]. Finally, (33), (34), (35), (44), and (45) give the closed-form expression (42) for the DNS throughput of an MWN in Nakagami-m fading channels. □

V. Case Study

We consider a case study with two-level wireless networks, for which we quantify both the DNS and the network lifetime. First, we describe the scenario and then provide the results in terms of DNS throughput and average number of rounds per node. The analysis is corroborated by simulation results for various network configurations.

A. Network Scenario and Performance Analysis

1) Network Scenario: We consider a scenario with a two-level ($L = 2$) legitimate network in $\mathbb{R}^2$, composed of non-GNs in level 2 and GNs in level 1. A two-level eavesdropping network is composed of eavesdropping nodes aiming to intercept information of non-GNs and GNs in levels 2 and 1, respectively, with spatial density $\lambda_{\mathrm{e}}^{(2)} = \lambda_{\mathrm{e}}^{(1)} = \breve{\lambda}_{\mathrm{e}}$. We consider Z_{T} channels available to transmitting nodes in a bounded space $\mathcal{B}_{\mathrm{o}}(r)$ with area $B(r) = \pi r^2$. Among the Z_{T} channels, $Z_2 = \delta_2 Z_{\mathrm{T}} = (1-\delta_1) Z_{\mathrm{T}}$ with $\delta_1 \in (0,1)$ and $Z_1 = \delta_1 Z_{\mathrm{T}}$ channels are available to legitimate nodes in level 2 and 1, respectively.

2) Distributed Network Secrecy: The DNS throughput in Nakagami-m fading channels depends on $p_{\mathrm{c}}^{(l)}$, determined by the MAC protocol, according to (42). In particular, we consider an access protocol according to which each legitimate node randomly selects a communication channel independently of other legitimate nodes in the same level [5]. Conditioned on the number n_l of transmitting nodes in level l, the probability that a node in level l transmits without collision is given by [61]

$$p_{\mathrm{c}}^{(l)}(n_l) = \left(1 - \frac{1}{Z_l}\right)^{n_l - 1}. \tag{46}$$

Therefore, the probability that a node in level l transmits without collision becomes

$$\begin{aligned} p_{\mathrm{c}}^{(l)} &= \mathbb{E}_{n_l}\left\{ p_{\mathrm{c}}^{(l)}(n_l) \right\} \\ &= \frac{Z_l e^{-N_{\mathrm{t}}^{(l)}/Z_l} - e^{-N_{\mathrm{t}}^{(l)}}}{Z_l - 1} \end{aligned} \tag{47}$$

where $N_{\mathrm{t}}^{(l)}$ is the average number of level l transmitting nodes in $\mathcal{B}_{\mathrm{o}}(r)$ as

$$N_{\mathrm{t}}^{(l)} = \pi r^2 \, p_{\mathrm{t}}^{(l)} \beta^{(l)} \lambda_\ell \, . \tag{48}$$

By using (47) and (48) in (42), we obtain the DNS throughput for Nakagami-m fading channels.

3) Network Lifetime: In each round, every node generates b_{g} bits to communicate its observation. For a given $R_\ell = W \log_2\left(1 + \check{\zeta}_\ell\right)$, each non-GN transmits $s_2 = b_{\mathrm{g}} / (R_\ell T)$ symbols per round. Thus, a typical GN transmits $(n_2 + 1) s_2$ symbols where n_2 is the number of non-GNs in a cluster whose transmission to the GN is successfully received without collision. The mean of n_2 is given by

$$\mathbb{E}\{n_2\} = \pi r_2^2 \, p_{\mathrm{ga}}^{(2)} \, p_{\mathrm{r}}^{(2)} \, p_{\mathrm{c}}^{(2)} \beta^{(2)} \lambda_\ell \, . \tag{49}$$

TABLE II
Parameter values if not otherwise specified

Parameters	Values	Parameters	Values
α	4	λ_ℓ	10^{-3}
m	1	$\breve{\lambda}_{\mathrm{e}}$	3×10^{-6}
WT	1	$\beta^{(1)}$	0.4
r_1, r [m]	100	$E_{\mathrm{b}}^{(2)}$ [J]	10^{-6}
r_2 [m]	30	E_{charged} [J]	10
b_{g}	2	Δ_1	30
b_{s}	1	δ_1	0.7

From (7) and (49), the average number of transmitted symbols per GN in a round results in

$$\begin{aligned} s_1 &= s_2 \, \mathbb{E}_{n_2}\{n_2 + 1\} \\ &= \frac{b_{\mathrm{g}}}{R_\ell T} \left[\frac{\beta^{(2)}}{\beta^{(1)}} \, p_{\mathrm{r}}^{(2)} \, p_{\mathrm{c}}^{(2)} \left(1 - e^{-\pi r_2^2 \beta^{(1)} \lambda_\ell}\right) + 1 \right]. \end{aligned} \tag{50}$$

Finally, by substituting (50) together with the expression for s_2 into (24), we obtain the network lifetime for a two-level wireless network as

$$\begin{aligned} N_{\mathrm{round}} = E_{\mathrm{charged}} \Bigg[E_{\mathrm{b}}^{(2)} b_{\mathrm{g}} \Bigg[& \beta^{(2)} p_{\mathrm{t}}^{(2)} + \Delta_1 \beta^{(1)} p_{\mathrm{t}}^{(1)} \\ & \times \left(\frac{\beta^{(2)}}{\beta^{(1)}} p_{\mathrm{r}}^{(2)} p_{\mathrm{c}}^{(2)} \left(1 - e^{-\pi r_2^2 \beta^{(1)} \lambda_\ell}\right) + 1 \right) \Bigg] \Bigg]^{-1}. \end{aligned} \tag{51}$$

B. Performance Evaluation

We now evaluate the performance of a two-level wireless network described in Sec. V-A. Unless otherwise specified, the values of network parameters presented in Table II are used.[14]

1) Distributed network secrecy: Figure 2 shows ρ_{ds} as a function of $E_{\mathrm{b}}^{(2)}$ for different values of Δ_1 and Z_{T} (ideal MAC refers to the case with no collision). Simulation results, depicted by circles, show a good agreement with the analysis. It can be seen that ρ_{ds} increases with $E_{\mathrm{b}}^{(2)}$ up to a maximum value, after which it decreases. This can be attributed to the competing effects of increasing $E_{\mathrm{b}}^{(2)}$, which increases the legitimate reception capability as well as the eavesdropping capability. Note also that ρ_{ds} increases with Z_{T} since collisions among nodes are less frequent with more available channels. It can also be observed from Fig. 2 that increasing Δ_1 increases ρ_{ds} when $E_{\mathrm{b}}^{(2)}$ is small, whereas the trend is opposite when $E_{\mathrm{b}}^{(2)}$ is large. This behavior is further investigated in the next figure.

Figure 3 displays the contour of ρ_{ds} as a function of $E_{\mathrm{b}}^{(2)}$ and Δ_1. It can be seen that the optimal value of Δ_1, which maximizes ρ_{ds}, decreases as $E_{\mathrm{b}}^{(2)}$ increases. This can be attributed to the fact that, when $E_{\mathrm{b}}^{(2)}$ is high, increasing the transmitted energy at GNs increases the eavesdropping capability more than the legitimate successful reception capability. Therefore, the joint optimization of parameters (e.g., energy ratio and transmitted bit energy) is important for designing

[14] For the considered parameters, ρ_{ds} can be thought of as the fraction of b_{s} confidential bits that each node successfully transmits with DNS per round.

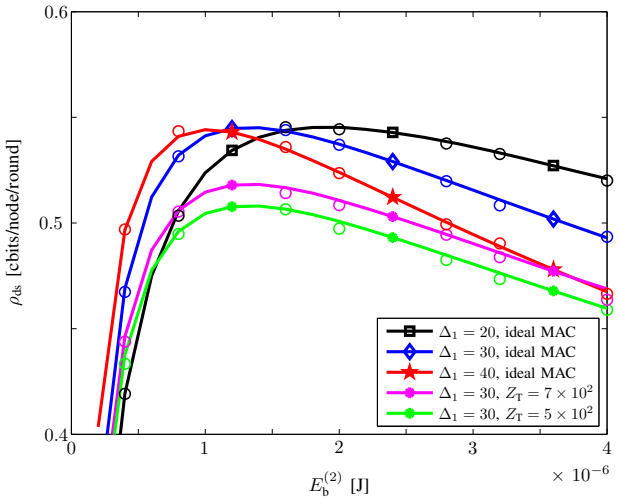


Fig. 2. ρ_{ds} as a function of $E_b^{(2)}$ for different values of energy ratio Δ_1 and number of available channels Z_T. Circle markers are for simulation results.

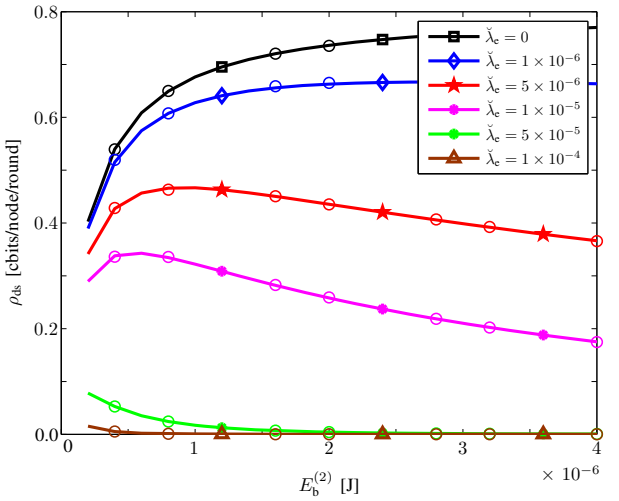


Fig. 4. ρ_{ds} as a function of $E_b^{(2)}$ for different values of eavesdropping node density $\breve{\lambda}_e$. Circle markers are for simulation results.

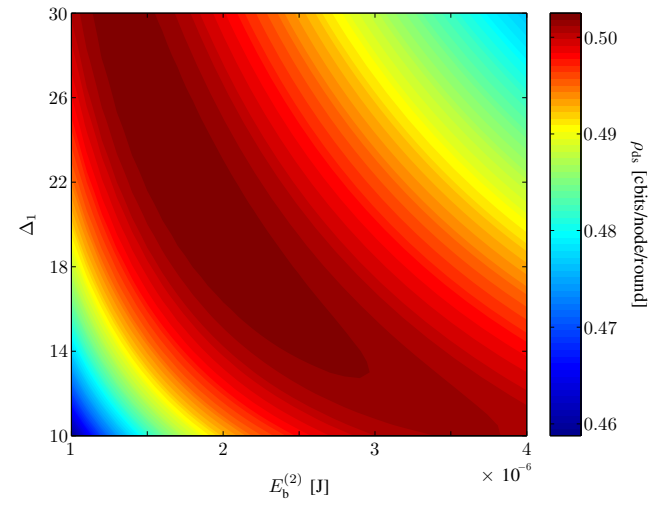


Fig. 3. ρ_{ds} as a function of $E_b^{(2)}$ and Δ_1.

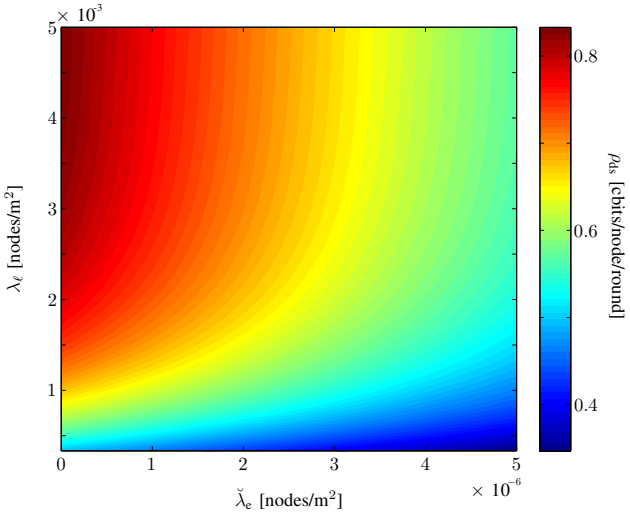


Fig. 5. ρ_{ds} as a function of $\breve{\lambda}_e$ and λ_ℓ.

MWNs with DNS. For instance, the maximum ρ_{ds} is achieved with $E_b^{(2)} = 1.6$ μJ and $\Delta_1 = 24$.

Figure 4 shows ρ_{ds} as a function of $E_b^{(2)}$ for different values of $\breve{\lambda}_e$ with no collision. Simulation results, depicted by circles, show a good agreement with the analysis. It can be seen that, in the absence of eavesdroppers ($\breve{\lambda}_e = 0$), ρ_{ds} increases with $E_b^{(2)}$ as expected since legitimate reception capability increases with $E_b^{(2)}$. In the presence of eavesdroppers, increasing $E_b^{(2)}$ above a certain value is harmful since the increase in eavesdropping capability outweigh the increase in the legitimate reception capability especially for large $\breve{\lambda}_e$.

Figure 5 displays the contour of ρ_{ds} as a function of $\breve{\lambda}_e$ and λ_ℓ. It can be seen that ρ_{ds} increases with λ_ℓ for a given $\breve{\lambda}_e$. This can be attributed to the fact that the legitimate transmission capability, from non-GN to its associated GN, increases with λ_ℓ. The increase in ρ_{ds} is more significant for smaller values of $\breve{\lambda}_e$, where legitimate transmission capability heavily outweigh the eavesdropping capability.

2) Network lifetime: Figure 6 shows N_{round} as a function of δ_1 for different Z_T. It can be seen that N_{round} increases with δ_1. This can be attributed to the fact that the energy consumption depends on both transmissions and collisions at level 2, and not on the collisions at level 1. In fact, smaller Z_2 (higher δ_1) induces more frequent collisions among non-GNs, and consequently a smaller amount of information is received from non-GNs, which reduces the energy consumption of GNs.

Figure 7 displays the contour of N_{round} as a function of $E_b^{(2)}$ and Δ_1. It can be seen that N_{round} becomes smaller as $E_b^{(2)}$ or Δ_1 increases due to higher energy consumption at each node. By comparing Figs. 3 and 7, it is evident that the optimal values of $E_b^{(2)}$ and Δ_1 that maximize ρ_{ds} do not maximize N_{round}. Therefore, it is important to jointly consider ρ_{ds} and N_{round} in designing energy-efficient MWNs with DNS. The relationship between ρ_{ds} and N_{round} is now explored.

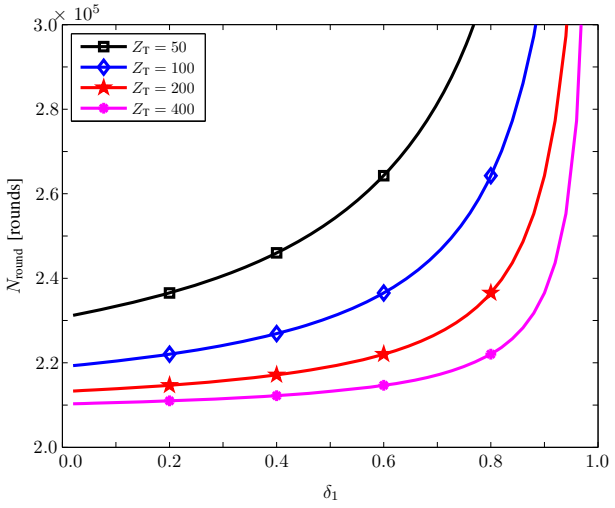


Fig. 6. N_{round} as a function of δ_1 for different number of total available channels Z_{T}.

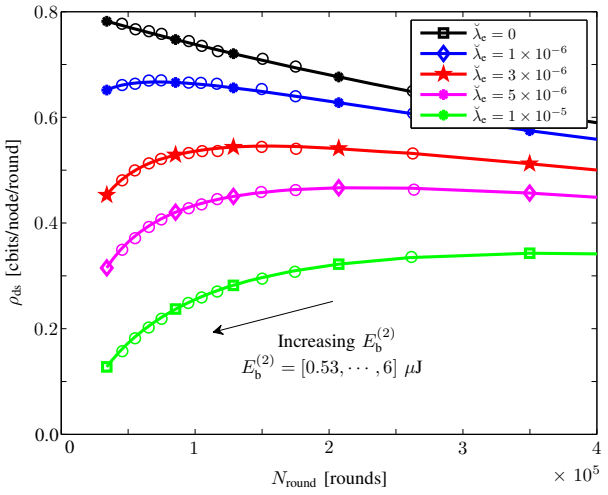


Fig. 8. ρ_{ds} as a function of N_{round} for different values of $\breve{\lambda}_{\text{e}}$ and $E_{\text{b}}^{(2)}$. Circle markers are for simulation results.

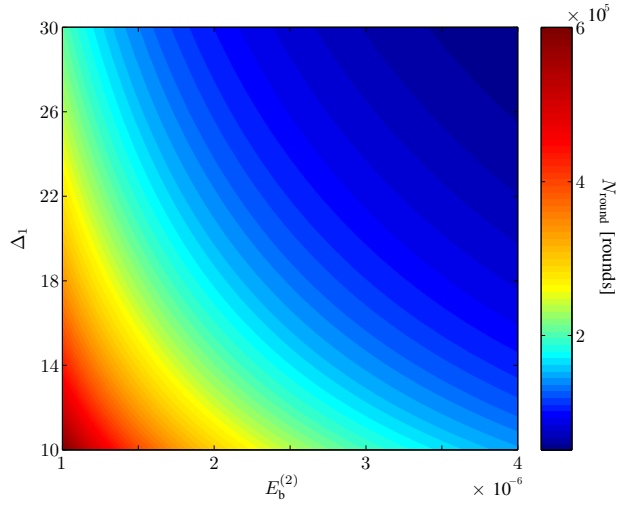


Fig. 7. N_{round} as a function of $E_{\text{b}}^{(2)}$ and Δ_1.

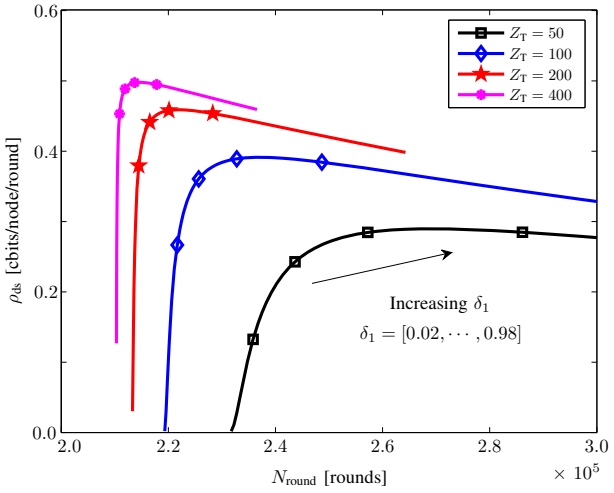


Fig. 9. ρ_{ds} as a function of N_{round} for different values of Z_{T} and δ_1.

3) Relationship between DNS and network lifetime: Figure 8 shows the relationship between ρ_{ds} and N_{round} for different values of $E_{\text{b}}^{(2)}$ and $\breve{\lambda}_{\text{e}}$. Simulation results, depicted by circles, show a good agreement with the analysis. For a given $E_{\text{b}}^{(2)}$, it can be seen that ρ_{ds} decreases as $\breve{\lambda}_{\text{e}}$ increases, while N_{round} is not affected by $\breve{\lambda}_{\text{e}}$. In the absence of eavesdropping nodes ($\breve{\lambda}_{\text{e}} = 0$), a trade-off between ρ_{ds} and N_{round} exists since ρ_{ds} increases while N_{round} decreases with increasing $E_{\text{b}}^{(2)}$. This relationship changes in the presence of eavesdropping nodes ($\breve{\lambda}_{\text{e}} > 0$) especially for large $\breve{\lambda}_{\text{e}}$ such as $\breve{\lambda}_{\text{e}} = 10^{-5}$ where both ρ_{ds} and N_{round} decrease as $E_{\text{b}}^{(2)}$ increases.

Figure 9 shows ρ_{ds} as a function of N_{round} for different values of Z_{T} and δ_1. It can be seen that ρ_{ds} increases and then, after a certain point, decreases while N_{round} always increases as δ_1 increases. Therefore, a trade-off between ρ_{ds} and N_{round} exists for large values of δ_1, whereas they both follow the same trend for small values of δ_1. This behavior of ρ_{ds} can be attributed to competing effects of increasing δ_1, which increases the capability of transmission without collision as well as the capability of eavesdropping the confidential information in level 1. In fact, collisions in level 1 reduce ρ_{ds} more than collisions in level 2, since each GN transmits $(n_2 + 1)b_{\text{s}}$ cbits while each non-GN transmits b_{s} cbits. On the other hand, collisions in level 2 reduce the amount of information transmitted and, therefore, the amount of information eavesdropped in level 1.

We now evaluate the achievable DNS throughput during the network lifetime, that is $\rho_{\text{ds}} \times N_{\text{round}}$, to measure the average number of confidential bits communicated per node during the network lifetime. Figure 10 shows $\rho_{\text{ds}} \times N_{\text{round}}$ as a function of $E_{\text{b}}^{(2)}$ and Δ_1. From this figure, it can be observed that lower Δ_1 achieves higher $\rho_{\text{ds}} \times N_{\text{round}}$ for all values of $E_{\text{b}}^{(2)}$, whereas from Fig. 3, lower Δ_1 does not necessarily achieve higher ρ_{ds} for varying $E_{\text{b}}^{(2)}$.

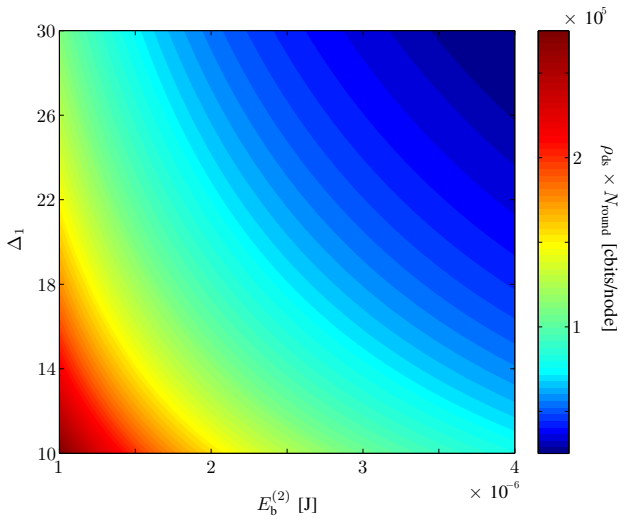


Fig. 10. $\rho_{ds} \times N_{round}$ as a function of $E_b^{(2)}$ and Δ_1.

VI. Conclusion

This paper introduces the concept of DNS and establishes a foundation for the network secrecy in self-organizing MWNs accounting for node spatial distribution, multilevel cluster formation, propagation medium, communication protocol, and energy consumption. By quantifying the DNS throughput and the energy consumption, we showed how network configurations influence both the DNS and the network lifetime. Specifically, our results demonstrate that different configurations of transmitted energy and communication resources induce different relationships between the DNS throughput and the network lifetime. The outcomes of our work provide guidelines for the design and analysis of reliable and energy-efficient self-organizing MWNs with DNS.

Acknowledgment

The authors wish to thank and W. Dai, Y. Shen, and T. Wang for the careful reading of the manuscript.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] M. Tubaishat and S. Madria, "Sensor networks: an overview," *IEEE Potentials*, vol. 22, no. 2, pp. 20–23, Apr./May 2003.

[3] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, vol. 4, Salt Lake City, UT, May 2001, pp. 2033–2036.

[4] S. Simić and S. Sastry, "Distributed environmental monitoring using random sensor networks," in *Proc. Workshop Information Processing in Sensor Networks*. Springer, Paolo Alto, CA, Apr. 2003, pp. 582–592.

[5] D. Dardari, A. Conti, C. Buratti, and R. Verdone, "Mathematical evaluation of environmental monitoring estimation error through energy-efficient wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 7, pp. 790–802, Jul. 2007.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[7] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] A. B. Carleial and M. E. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[9] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[10] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[11] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[12] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[13] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764 –2775, Aug. 2011.

[14] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[15] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs under passive and active attacks," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6692–6702, Oct. 2011.

[16] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[17] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[18] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 1–10, Jan. 2010.

[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[20] ——, "Secret communication in presence of colluding eavesdroppers," in *Proc. Military Commun. Conf.*, Atlantic City, NJ, Oct. 2005, pp. 1501–1506.

[21] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forens.Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[22] O. Koyluoglu, C. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[23] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[24] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. on Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 524–528.

[25] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[26] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[27] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[28] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[29] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[30] Y. Shen and M. Z. Win, "Intrinsic information of wideband channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, Sep. 2013.

[31] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[32] W. Saad, Z. Han, T. Başar, M. Debbah, and A. Hjørungnes, "Distributed coalition formation games for secure wireless transmission," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 231–245, Apr. 2011.

[33] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.

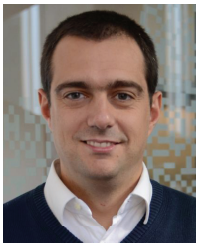
[34] M. Z. Win, "A mathematical model for network interference," *IEEE Communication Theory Workshop*, Sedona, AZ, May 2007.

[35] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009.

[36] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless network," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
[37] J. Orriss and S. K. Barton, "Probability distributions for the number of radio transceivers which can communicate with one another," *IEEE Trans. Commun.*, vol. 51, no. 4, pp. 676–681, Apr. 2003.
[38] E. Salbaroli and A. Zanella, "Interference analysis in a Poisson field of nodes of finite area," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1776–1783, May 2009.
[39] A. Rabbachin, T. Q. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.
[40] E. S. Sousa, "Performance of a spread spectrum packet radio network link in a Poisson field of interferers," *IEEE Trans. Inf. Theory*, vol. 38, no. 6, pp. 1743–1754, Nov. 1992.
[41] A. Ghasemi and E. S. Sousa, "Interference aggregation in spectrum-sensing cognitive wireless networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 41–56, Feb. 2008.
[42] P. C. Pinto and M. Z. Win, "Communication in a Poisson field of interferers – Part I: Interference distribution and error probability," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2176–2186, Jul. 2010.
[43] ——, "Communication in a Poisson field of interferers – Part II: Channel capacity and interference spectrum," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2187–2195, Jul. 2010.
[44] J. Ilow, D. Hatzinakos, and A. N. Venetsanopoulos, "Performance of FH SS radio networks with interference modeled as a mixture of Gaussian and alpha-stable noise," *IEEE Trans. Commun.*, vol. 46, no. 4, pp. 509–520, Apr. 1998.
[45] X. Yang and A. P. Petropulu, "Co-channel interference modeling and analysis in a Poisson field of interferers in wireless communications," *IEEE Trans. Signal Process.*, vol. 51, no. 1, pp. 64–76, Jan. 2003.
[46] S. Govindasamy, D. W. Bliss, and D. H. Staelin, "Spectral efficiency in single-hop ad-hoc wireless networks with interference using adaptive antenna arrays," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 7, pp. 1358–1369, Sep. 2007.
[47] J. Lee, J. G. Andrews, and D. Hong, "Spectrum-sharing transmission capacity," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3053–3063, Sep. 2011.
[48] P. C. Pinto and M. Z. Win, "Percolation and connectivity in the intrinsically secure communications graph," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1716–1730, Mar. 2012.
[49] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. on Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 539–543.
[50] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.
[51] A. Rabbachin, A. Conti, and M. Z. Win, "The role of aggregate interference on intrinsic network secrecy," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012, pp. 3548–3553.
[52] J. Lee, H. Shin, and M. Z. Win, "Secure node packing of large-scale wireless networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012, pp. 815–819.
[53] J. F. Kingman, *Poisson Processes*. Oxford University Press, 1993.
[54] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*. Dover Publications, 1970.
[55] J. Gil-Pelaez, "Note on the inversion theorem," *Biometrika*, vol. 38, no. 3/4, pp. 481–482, Dec. 1951.
[56] R. Verdone, D. Dardari, G. Mazzini, and A. Conti, *Wireless Sensor and Actuator Networks: Technologies, Analysis and Design*. Elsevier, 2008.
[57] F. Zhao, J. Liu, J. Liu, L. Guibas, and J. Reich, "Collaborative signal and information processing: an information–directed approach," *Proc. IEEE*, vol. 91, no. 8, pp. 1199–1209, Aug. 2003.
[58] A. Conti, W. M. Gifford, M. Z. Win, and M. Chiani, "Optimized simple bounds for diversity systems," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2674–2685, Sep. 2009.
[59] F. Baccelli and B. Błaszczyszyn, *Stochastic Geometry and Wireless Networks, Volume I — Theory*, ser. Foundations and Trends in Networking. NoW Publishers, 2009.
[60] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*. Wiley-IEEE Press, 2004.
[61] Leon-Garcia and I. Widjaja, *Communication Networks: Fundamental Concepts and Key Architectures*. McGraw-Hill, 2000.

Jemin Lee (S'06-M'11) is a Postdoctoral Fellow at the Massachusetts Institute of Technology since 2010 and a Research Fellow at Singapore University of Technology and Design since 2013. Her research interests involve communication theory and stochastic geometry applied to cognitive radio networks, heterogeneous wireless networks, and network secrecy. Dr. Lee is a Guest Editor for the ELSEVIER Physical Communication and in the organization of numerous international conferences. She has been recognized as an exemplary reviewer of the IEEE Communication Letters. She received the Chun-Gang Outstanding Research Award and fellowship from National Research Foundation of Korea.

Andrea Conti (S'99-M'01-SM'11) is a Professore Aggregato at the University of Ferrara. He also holds Research Affiliate appointments at IEIIT, Consiglio Nazionale delle Ricerche, and at LIDS, Massachusetts Institute of Technology. His research interests involve theory and experimentation of wireless systems and networks including network localization, adaptive diversity communications, cooperative relaying techniques, and network secrecy. Dr. Conti is serving as an Editor for the IEEE Communications Letters and served as an Associate Editor for the IEEE Transactions on Wireless Communications. He is elected Chair of the IEEE Communications Society's Radio Communications Technical Committee and is an IEEE Distinguished Lecturer. He is a recipient of the HTE Puskás Tivadar Medal and is co-recipient of the IEEE Communications Society's Fred W. Ellersick Prize and of the IEEE Communications Society's Stephen O. Rice Prize in the Field of Communications Theory.



Alberto Rabbachin (S'03-M'07) is a Postdoctoral Fellow at the Massachusetts Institute of Technology. His research interests involve communication theory and stochastic geometry applied to real-problems in wireless networks including network secrecy, cognitive radio, ultrawide band transceiver design, network synchronization, ranging techniques, and interference exploitation. Dr. Rabbachin serves as an Editor for the IEEE Communications Letters and in the organization of numerous international conferences. He received the International Outgoing Marie Curie Fellowship, the Nokia Fellowship, the European Commission JRC best young scientist award, and the IEEE William R. Bennett Prize in the Field of Communications Networking.

Moe Z. Win (S'85-M'87-SM'97-F'04) is a Professor at the Massachusetts Institute of Technology (MIT) and the founding director of the Wireless Communication and Network Sciences Laboratory. Prior to joining MIT, he was with AT&T Research Laboratories and with the Jet Propulsion Laboratory. His research encompasses developing fundamental theories, designing algorithms, and conducting experimentation for a broad range of real-world problems. Dr. Win is a Fellow of the AAAS and of the IEEE. He is an elected Member-at-Large on the IEEE Communications Society Board of Governors. He served as Editor for various IEEE journals and chaired a number of international conferences. He received the Fulbright Fellowship, the Copernicus Fellowship, and the Laurea Honoris Causa from the University of Ferrara. Together with students and colleagues, his papers have received several awards including the IEEE Communications Societys Stephen O. Rice Prize, the IEEE Aerospace and Electronic Systems Societys M. Barry Carlton Award, and the IEEE Antennas and Propagation Societys Sergei A. Schelkunoff Transactions Prize Paper Award. He was honored with the IEEE Kiyo Tomiyasu Award and the IEEE Eric E. Sumner Award.