Malicious Relay Detection Using Sentinels: A Stochastic Geometry Framework

Utku Tefek, Anshoo Tandon, and Teng Joon Lim

Abstract: **Next generation wireless networks are under high risk of security attacks due to increased connectivity and information sharing among peer nodes. Some of the nodes could potentially be malicious, intending to disrupt or tamper sensitive data transfer in the network. In this paper, we present a detailed analysis of the sentinel based data integrity attack detection of malicious relays using a stochastic geometry framework. We assume a practical channel model for each wireless link and apply a stochastic geometry approach to interference modeling. Two detection schemes depending on the level of connectivity between sentinel devices are proposed: isolated and co-operative detection. For both schemes, attack detection probability is derived as a function of important network parameters, and the minimum density of sentinels to achieve a given detection probability is calculated. It will be shown that a reasonable attack detection probability can be achieved even when the sentinel node density is much lower than the relay node density.**

Index Terms: **Attack detection, internet-of-things, sentinel, stochastic geometry**

I. INTRODUCTION

WIRELESS communication networks comprising many interconnected nodes are vulnerable to disruption or corruption of vital information by malicious nodes present in the network. Securing these networks can be very difficult because the attack surface can be enormous. Any device in the network can be a potential entry point via exposed serial ports, physical tampering, hard-coded keys and credentials, insecure wireless communications and applications. The data contained in the network may be sensitive or valuable, entailing huge potential gains for the attacker that hinders data transmission, steals information and/or modifies data.

Conventionally, security schemes are developed mostly for the upper layers of the network, with a focus on cryptography-based methods. For example, data integrity can be ensured by message authentication codes or digital signatures. However, the low hardware complexity and energy consumption requirements of IoT devices pose a challenge to adopt computationally exhaustive algorithms [1]. Additionally, the management of secret keys often requires complex protocols and architectures, rendering the cryptography-based methods difficult to implement in large IoT networks [2].

In this paper, we consider a hierarchical wireless network architecture, a typical setup in IoT, in which a group of IoT devices connects to an access point (AP) through another wireless node known as a gateway or relay. The clustering of nodes results in relays becoming higher value targets since a relay can easily disrupt the communication of all the devices it serves. The attack model assumes that the compromised relays may either alter, drop or artificially craft data packets. We adopt the sentinel based security scheme proposed in [3] to detect such data integrity attacks initiated by IoT relays. Sentinels are special passive nodes, sniffing data packets transmitted by both IoT devices and relays, by exploiting the broadcast nature of wireless transmissions. The proposed detection system is based on having sentinels compare the MAC layer payloads transmitted by the devices and their associated relays, which should be identical because the relays are only forwarding the IoT packets. Taking the wireless communication characteristics of the transmissions into account (e.g., possible outages due to bad channel conditions and interference), the sentinels detect relays engaged in such malicious activity with the desired probability. Unlike [3], [4], which assume known channel parameters, here we take a stochastic geometry approach to analyze the detection performance.

A. Related Work

A cross-layer approach to the detection of malicious relays in a two-hop wireless network was presented in [5], but its operation assumed that some devices forward the same information through two different relays. In [6], a channel-aware scheme for selective forwarding attack detection is proposed, but it has the drawback of high missed detection probability in case only a small fraction of packets are dropped by a malicious node. Detection of false data injection attacks by a malicious relay via physical layer techniques was presented in [7], [8]. In [7], the detection scheme operated at the modulated symbol level, but the detection performance degraded significantly in scenarios where the end-to-end channel gain between the source and the final destination is small. In [8], a Bayesian test approach at the packet level is proposed, but the performance is unsatisfactory when the relay corrupts only a small fraction of bits.

In [9], the use of received signal strength indicator readings was proposed for the detection of selective forwarding attacks. However, this method relied on a sophisticated localization algorithm for estimating the distances among nodes. The use of a checkpoint node along the forwarding path was proposed in [10] for the detection of selective forwarding attack. This scheme, however, requires major changes to existing wireless sensor network protocols, including implementation of one-way hash

Manuscript received September 5, 2019; revised February 29, 2020; approved for publication by Division II Editor Wonjun Lee, May 4, 2020.

U. Tefek is with the Advanced Digital Sciences Center, Singapore, email: u.tefek@adsc-create.edu.sg.

A. Tandon is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, email: anshoo.tandon@gmail.com.

T. J. Lim is with the School of Electrical and Information Engineering, University of Sydney, Australia, email: tj.lim@sydney.edu.au.

Digital Object Identifier: 10.1109/JCN.2020.000010

functions and the exchange of ACK packets with timing information.

An overhearing-based approach to malicious node detection was proposed in [11], where each node is expected to report the packet forwarding ratio for its neighbors. This approach, however, results in heavy computational load on the network resources, as every device continuously monitors the information exchanged with neighboring nodes. In [12], a similar approach was adopted, and nodes were assumed to monitor their two-hop neighbors. A watchdog technique for data integrity attack detection was presented in [13], but it does not consider packet loss due to channel noise, and also suffers from the heavy computational load as each node is expected to monitor its neighboring node. In [14], the destination detects Byzantine attacks by observing certain signals containing side information, which cannot be altered by the malicious relay. We remark that an important distinction between our sentinel based malicious detection, and previous works based on watchdog approach [11]–[13], is that the sentinel based detection scheme *does not require any changes to standard wireless/IoT protocols*: The task of monitoring and reporting malicious behavior is entrusted *only* to secure sentinel nodes which are placed appropriately by the network designer.

In [15], a malicious relay detection scheme, operating in the absence of a reference signal at the receiver, was presented for an amplify-and-forward relay network. This scheme exploited the knowledge of channel characteristics, but the system was analyzed only in an asymptotic setting with an extremely large number of symbols required for detection. In a similar amplify-and-forward relay setting presented in [16], a novel approach to detect the malicious relays engaged in false information forwarding in the presence of unreliable CSI is proposed. However, not all types of false forwarding and dishonest CSI feedback attacks can be detected, especially when there is no direct link between the source and the destination.

The overhearing/watchdog-based relay detection schemes in the above-mentioned papers either did not consider the outage characteristics or assumed fixed received interference and signal powers to calculate the outage probability. In fact, the perceived signal powers and the interference from concurrent transmissions at the sniffer nodes (sentinels) depend on the network geometry. A significant difference in our scheme is its ability to model the network geometry to accurately capture the outage characteristics. This is achieved through the use of stochastic geometry modelling which has been successfully adopted in heterogeneous [17]–[19] and IoT/machine-to-machine relay networks [20]–[22]. For example, the optimal partitioning of spectrum resources into IoT devices and relay nodes to maximize the density of supported IoT devices has been addressed in [20]. The analysis of resource scheduling strategies at the relay nodes has been studied in [21]. A multi-hop data aggregation scheme to minimize the energy density of an IoT network has been proposed in [22].

Stochastic geometry has also been used in a number of papers studying physical layer security. In [23], secure communication in a cognitive radio network, in the presence of randomly distributed eavesdroppers has been studied. Based on various channel knowledge assumptions at the transmitter, transmission protocols have been designed to achieve secure transmission. In [24], [25], interference from the secondary users of a random cognitive radio network is exploited as artificial noise to improve the secrecy throughput of the primary network. In [26], two secrecy improvement techniques namely, creating guard zones and adding artificial noise have been comparatively analyzed using stochastic geometry. In [27] the secrecy performance of a primary network overlaid with an RF energy harvesting secondary IoT network has been studied. Assuming that the secondary network is solely powered by the ambient RF energy harvested from the transmissions of the primary network, the optimal deployment density for the secondary network for maximal energy harvesting has been calculated under secure communication constraints. As discussed, the earlier works on stochastic geometry focused on beamforming design [28], [29] to improve secrecy in various scenarios and proposed useful optimizations secrecy. In this paper, we focus on another aspect of secure communications, which is message integrity.

Our proposed scheme complements cryptography-based approaches as an additional defense mechanism, because the limited processing capabilities of resource-constrained devices may not be relied upon to support a desired level of security. Additionally, cryptography-based detection of data integrity attack has the limitation that it cannot locate the malicious relay node in multi-hop networks [30].

B. Contributions

This paper proposes a stochastic geometry framework to analyze the detection probability of data integrity attacks launched by relays in an IoT network. In particular, the locations of the devices, relays, APs, and sentinels are represented as point processes with certain densities. Stochastic geometry modeling allows us to calculate the interference and signal power distributions and thus to derive the outage probability of each link averaged over the space of all network realizations.[1] Then, the minimum density of sentinels which ensures a certain detection probability is calculated. The analysis is performed for two detection models, named based on the degree of communication among sentinels: isolated detection and co-operative detection. Further details on the system model are provided in the following section.

The distinguishing features of our proposed scheme, and the resulting analysis are as follows.

1. Our model considers a practical scenario where different wireless links in the network may have different packet error probabilities depending on their channel conditions. As such, some transmissions may be unsuccessful, and the probability of sentinels capturing a certain packet is a function of the network geometry.
2. Unlike the majority of physical layer security schemes, our model does not assume known channel parameters or node locations for the design. Thanks to the use of stochastic geometry, the obtained results are the averages over the space of all possible network realizations. Thus, the presented

[1] The outage in device-to-relay and relay-to-AP links refer to a failed decoding attempt, whereas in device-to-sentinel and relay-to-sentinel links, it is the failure of the associated sentinel(s) to sniff and decode the packet.

communication theoretical results serve as a baseline for the design of future sentinel based detection schemes.

3. The proposed detection scheme imposes no additional burden on the resource-constrained IoT devices and relays, but rather passively monitors them for anomalies through the passive sentinel nodes. The network operator is notified only when an anomaly is detected. While adding sentinels comes with additional hardware and maintenance costs, as will be shown through analysis, a respectable attack detection probability can be achieved even when the sentinel node density is much lower than the relay node density. This is a critical advantage over other schemes, which typically require additional computations on the part of IoT devices.
4. The probability of false alarm in our detection scheme is negligible. We remark that a false alarm occurs only in the unlikely scenario where the packet cyclic redundancy check (CRC) fails to *detect* errors in the decoded packet (after error correction), even though the decoded packet is in error. Therefore, the false alarm probability in our detection scheme can be made negligible by using a sufficiently long CRC. This is distinct from previously proposed detection schemes which trade probability of missed detection against the probability of false alarm.

II. SYSTEM MODEL

A. Network Model

Consider a wireless IoT network where IoT devices connect to the APs only via wireless decode-and-forward relays. The locations of devices, relays, APs and sentinels are assumed to follow four independent homogeneous spatial Poisson point processes (PPPs), $\Phi_D = \{D_i\}$, $\Phi_R = \{R_i\}$, $\Phi_A = \{A_i\}$ and $\Phi_S = \{S_i\}$ with densities λ_D, λ_R, λ_A and λ_S respectively (Fig. 1). Each device is associated to its nearest relay and each relay is linked to its nearest AP, which also perceives the strongest average received power. Therefore, the spatial tessellation formed by the association regions of relays and access points can be characterized as two independent Poisson Voronoi tessellations [31]. The boundaries of relay association regions are shown in Fig. 1 by solid blue lines. Each relay listens to the devices within its own association region. Similar association regions are formed for linking relays to the APs, but this is not displayed in Fig. 1 for clarity. The sentinel association depends on the type of detection model employed.

1. *Isolated Detection:* In this model, the sentinels are unable to communicate with each other (excluding the initial association region setup) and have to detect the attacks individually. Therefore, a sentinel must overhear the transmissions of both a relay and other devices associated with this relay, in order to assess the malicious activity of this relay cluster. For maximal detection performance, each relay shall be associated with the sentinel which receives the relay's transmission with the highest average signal power. All the devices linked to a particular relay are monitored by the same sentinel. For instance, if the sentinel located at S_0 is the nearest sentinel to the relay located at R_0, all devices linked to this relay at R_0 would also be associated with S_0 even though S_0 is not necessarily the nearest sentinel to these devices. Such an association rule is necessary for the sentinel to overhear both the device's and its associated relay's transmissions of a particular data packet.
2. *Co-operative Detection:* If the sentinels can communicate with each other in the detection process, the detection performance improves. It is assumed that the transmitted device and relay packets are captured by a sentinel whenever the observed signal-to-interference ratio (SIR) exceeds a required value. Then, the device and relay versions of the sniffed packets with the identical sequence number and source ID are compared among sentinels to verify data integrity. Cooperative detection is able to detect packet modifications by the relay even when disjoint sets of sentinels capture a packet transmitted from a device and the same packet forwarded by the relay. In such a scenario, isolated detection would fail. It should be noted that instead of transmitting the whole sniffed packet for comparison, sentinels can compute and share only the checksums of MAC payloads, along with the source ID and sequence numbers to label the checksums. This would reduce the signaling overhead and allow a more robust error correction scheme for sentinel transmissions.

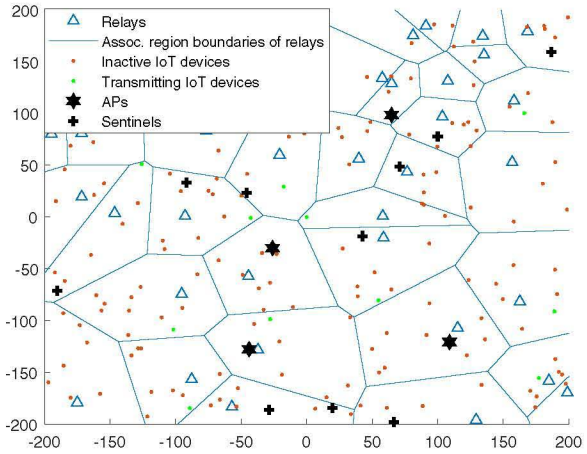

Fig. 1. A wireless IoT relay network with sentinel nodes. Note that only the association regions of relays are displayed. A similar Poisson Voronoi tessellation is formed by APs, and sentinels (in isolated detection).

We assume that the APs (relays) schedule their linked relays (devices) by assigning each relay (device) a different time slot, i.e., time division multiple access (TDMA). Hence, no more than one relay (device) can transmit within an association region of each AP (relay) in the same time slot. While we perform the analysis for a certain frequency channel, the analysis applies in the same way to other orthogonal frequency channels. In-active and transmitting IoT devices are labeled separately in Fig. 1. Note however that, multiple relays (devices) within different APs' (relays') association regions can transmit concurrently, thus causing mutual interference. The resulting spatial point processes of concurrently transmitting devices and relays are denoted by Φ_D^a and Φ_R^a, where $\Phi_D^a \subset \Phi_D$ and $\Phi_R^a \subset \Phi_R$. We denote the effective density of transmitting devices by $\lambda_D \delta_D$

and relays by $\lambda_R \delta_R$ where δ_D and δ_R are the fractions of devices and relays, respectively, which transmit in a time slot.[2] It is further assumed that the devices and relays transmit in orthogonal channels, therefore, no device-to-AP or relay-to-relay interference is present.

B. Channel Model

The transmitting devices and relays transmit with powers denoted by P_D and P_R respectively. The propagation model accounts for the path loss attenuation and large scale fading. For any transmitter located at X and receiver at Y, the path attenuation from X to Y is given by $\|Y - X\|^{-\alpha}$, where $\|Y - X\|$ is the distance between X and Y, and α denotes the path-loss exponent. The fading power gain from X to Y is denoted by $h_{Y,X}$. We assume that $\{h_{Y,X}\}$'s are unit mean exponential random variables (Rayleigh fading), independent across $\{X\}$ and $\{Y\}$s and transmission cycles. Received signals can be decoded only if they are received with SIR above a certain threshold η. I.e., for a transmitting node at $X \in \{\Phi_D \cup \Phi_R\}$, the probability of its intended receiver at $Y \in \{\Phi_R \cup \Phi_S \cup \Phi_A\}$ successfully capturing its packet is,

$$1 - \epsilon_{X \to Y} = \Pr\left(\frac{P_X h_{Y,X} \|Y - X\|^{-\alpha}}{I_Y} \geq \eta\right), \quad (1)$$

where $\epsilon_{X \to Y}$ is the outage probability from X to Y and I_Y is the aggregate interference received at Y.

C. Attack Model and Detection

The threat model and the sentinel based detection model are discussed in the following. Then, the attack detection probability is formulated as a performance metric.

It can be safely assumed that a unique source ID (e.g., MAC address) and a sequence number are associated with packets transmitted from each IoT device. The MAC layer also adds cyclic redundancy check (CRC) bits to the packet before passing it to the physical layer for error control coding and modulation. For a given packet transmission from device D_j to relay R_i, if the CRC fails at R_i due to interference and noise, then R_i does not send back an acknowledgment to D_j, and the packet with the same source ID, sequence number and payload has to be re-transmitted by D_j until an acknowledgment is received from R_i. Each relay node first demodulates and decodes the received physical layer signal using a suitable error control and/or correction scheme. Upon successfully decoding the packet, the relay keeps the source ID and sequence number in the header, adds its own ID, and passes the data to the physical layer for error control coding and modulation. Similarly, if CRC fails at the AP when decoding the packet transmitted by the relay R_i, the AP does not send an acknowledgment, demanding a re-transmission from the relay R_i. Acknowledgment packets are small and encoded with a robust error correction scheme so that they are received error-free.

The relays can be compromised due to several vulnerabilities including but not limited to default, weak or hard-coded credentials/keys, exposed serial ports, insecure wireless communications and applications, and physical tampering. Furthermore, the limited processing capabilities of IoT devices render the use of strong cryptography-based authentication and integrity checks uncommon, thus allowing the compromised relay node to tamper with the data packets undetected. In the absence of an appropriate attack detection mechanism, the adversary may inject malicious commands or false data, deny critical data transmissions for a prolonged duration, and even use the compromised relay node as an entry point to reach the susceptible parts of a cyber-physical system. In line with these potential risks, our attack model assumes that the compromised relay nodes either i) alter, ii) drop or iii) artificially craft data packets prior to relaying. The sentinels aim to detect the presence of a malicious relay node engaged in any of the three integrity attacks.

1. *Altering the payload*: The relay modifies the payload prior to transmission. The sentinels detect such attacks if they can successfully capture the corresponding packets (identical source ID and sequence number) transmitted by the IoT device and the relay.
2. *Dropping packets*: The relay intentionally drops some of the received packets instead of forwarding them to the AP, and also tampers with the sequence numbers such that the AP receives packets with consecutive sequence numbers. Note that, if the sequence numbers are not modified, the AP notices the missing sequence numbers. For instance, after correctly forwarding packets with sequence number $1, \ldots, i$, the compromised relay may drop the $(i+1)$'st packet, and forward the $(i+k)$'th packet with the tampered sequence number of $i + k - 1$ for $k = 1, 2, \ldots$. Such an attack can be detected if the sentinels can capture and compare any of the $(i+k)$'th packet from the device, and the packet labeled with sequence number $i + k$ from the relay.
3. *Crafting packets*: The compromised relay may craft a packet with spoofed source/destination ID and sequence number to test the presence, functionality or the accuracy of intrusion detection systems. If the source/destination ID and sequence numbers of the forged packet do not match the expected headers by the AP, then the attack can be readily detected by the AP. To avoid detection by the AP, the relay has to attach an appropriate source ID and the subsequent sequence number for that source, then send it to the AP as if it originated from an IoT device. The sentinels can detect such forged packets if they can capture both the forged packet and the corresponding authentic packet transmitted by the device, whose source ID and sequence number match that of the forged packet.

Note that all three types of integrity attacks can be detected if the sentinels capture at least two packets, one transmitted by the device and another from the relay whose source ID and sequence number match that of the device. Due to the proximity of a device to its associated relay induced by the Poisson Voronoi tessellation of the relays, there would be a weak correlation in the signal power from a device and its associated relay perceived at the typical sentinel. Nevertheless, this correlation would be limited because the device can still be located anywhere within the Poisson Voronoi cell with a uniform probability distribution, and

[2] Provided that $\lambda_D \delta_D \leq \lambda_R$ and $\lambda_R \delta_R \leq \lambda_A$, to ensure a considerable capture probability. This means, no more than a single device (relay) is transmitting within the association region of a relay (AP).

also because the channel gains are independent. Motivated by this argument, the detection probability of an attack is assumed to be the product of the probabilities of successfully capturing a typical device and a typical relay packet, or

$$p_d = (1 - \epsilon_{R \to S})(1 - \epsilon_{D \to S}), \tag{2}$$

where $\epsilon_{D \to S}$ and $\epsilon_{R \to S}$ are the outage probabilities when decoding a device and relay transmission, respectively.

D. Effects of Re-transmissions on the Detection Performance

As stated above and in line with conventional MAC protocols, re-transmissions are triggered until the appropriate acknowledgment packet is received in both device-to-relay and relay-to-AP links. When a transmission is repeated, the sentinels can capitalize on multiple opportunities to sniff the packet, improving the detection performance. For instance, if a relay node requests a re-transmission from its associated device before tampering with the data and relaying, it is sufficient for the sentinels to capture the malicious packet by the relay and either one of the transmitted packets from the device. Thus, $(1 - \epsilon_{D \to S})$ in (2) would have to be replaced by a higher probability, measuring the event that sentinels capture at least one of the device transmissions. However, we argue that the malicious relays may be smart enough not to request re-transmissions when they intend to alter the payload. To minimize the risk of being detected, a compromised relay may choose not to request re-transmissions for the packets whose source and sequence ID matches the malicious packets that it injects. Similarly, the compromised relay may choose not to transmit the malicious packet more than once if acknowledgment is not received from its associated AP. Therefore, the detection probability metric should not account for re-transmissions.

III. OUTAGE ANALYSIS

In this section, using stochastic geometry, we derive the outage probabilities for all four wireless links: device-to-relay ($\epsilon_{D \to R}$), relay-to-AP ($\epsilon_{R \to A}$), device-to-sentinel ($\epsilon_{D \to S}$) and relay-to-sentinel ($\epsilon_{R \to S}$). For the outage analysis, we condition on a typical receiving node and its tagged transmitter. Then, we express the received interference distribution and thus the probability of outage conditioned on the locations of this transmitter/receiver pair. Finally, we integrate the conditional outage probability over the distance distribution of the typical transmitter/receiver pair to obtain the average outage probability.

A. Communication Links: Device-to-Relay and Relay-to-AP

Since the same node association rule applies for device-to-relay and relay-to-AP wireless links, here we develop a Theorem which characterizes the received interference distribution from PPP distributed transmitters, when the typical transmitter (device or relay) is scheduled to transmit to its nearest receiver (relay or AP respectively). Then, using this Theorem, the capture probabilities of device-to-relay and relay-to-AP links can be obtained thanks to the PPP approximation on the locations of active transmitters.

Without loss of generality, let us assume that the typical receiver at Y_0, selected among the homogeneous PPP distributed receivers Φ_Y of density λ_Y, is located at the origin. As per the association rule of transmitter/receiver pairs, the association region of this typical receiver can be defined as a Poisson Voronoi cell [31],

$$\mathcal{V}_{Y_0} = \{X \in \mathbb{R}^2 : \|X - Y_0\| \leq \|X - Y_i\|, \forall Y_i \in \Phi_Y \backslash \{Y_0\}\}. \tag{3}$$

Let the interfering transmitter process $\Phi_X \backslash \mathcal{V}_{Y_0}$ be a homogeneous PPP with density λ_X outside the association region of the typical receiver. Also let $X_0 \in \Phi_X \cap \mathcal{V}_{Y_0}$ be the location of a tagged (marked) active transmitter of the typical receiver, uniformly distributed in $\mathcal{V}_{Y_0}$[3]. Given constant transmit powers of P_X and i.i.d unit mean exponential channel fading gains of $h_{Y_0,X}$ for all $X \in \Phi_X$, the received interference power at Y_0 is

$$I_{Y_0} = \sum_{X \in \Phi_X \backslash \mathcal{V}_{Y_0}} P_X h_{Y_0,X} \|X\|^{-\alpha}. \tag{4}$$

The following Theorem characterizes the Laplace transform of the distribution of I_{Y_0} and the capture probability at a typical receiver.

Theorem 1. Laplace transform of the interference distribution at the typical receiver is

$$\mathcal{L}_{I_{Y_0}}(s) = \exp\left\{-\pi\lambda_X \mathbb{E}_\rho\left[\rho^2 C_\alpha\left(sP_X\rho^{-\alpha}\right)\right]\right\}, \tag{5}$$

and the capture probability at this typical receiver is,

$$\begin{aligned}\mathcal{C}(\lambda_X, \lambda_Y, \eta, \alpha) &:= 1 - \epsilon_{X \to Y_0} \\ &= 2\pi\lambda_Y \int_0^\infty \exp\left\{-\pi\lambda_X \mathbb{E}_\rho\left[\rho^2 C_\alpha\left(\eta r^\alpha \rho^{-\alpha}\right)\right]\right\} \\ &\qquad \times \exp\left(-\pi\lambda_Y r^2\right) r \mathrm{dr}, \end{aligned} \tag{6}$$

where $C_\alpha(\theta) = \int_1^\infty \frac{\mathrm{dt}}{1+\theta^{-1}t^{\alpha/2}}$ and ρ is Rayleigh distributed with parameter $(2\pi\lambda_Y)^{-1/2}$.

Proof: The proof is given in Appendix A.

When $\alpha = 4$, the results in Theorem 1 can be further simplified as follows.

Corollary 1. If $\alpha = 4$,

$$\mathcal{L}_{I_{Y_0}}(s) = \exp\left\{-\pi\lambda_X\sqrt{sP_X}\left[\frac{\pi}{2} - \mathcal{A}(\pi\lambda_Y\sqrt{sP_X})\right]\right\}, \tag{7}$$

$$\begin{aligned}\mathcal{C}(\lambda_X, \lambda_Y, \eta, 4) &:= 1 - \epsilon_{X \to Y_0} \\ &= 2\pi\lambda_Y \int_0^\infty \exp\left\{-\pi\lambda_X\sqrt{\eta}r^2\left[\frac{\pi}{2} - \mathcal{A}(\pi\lambda_Y\sqrt{\eta}r^2)\right]\right\} \\ &\qquad \times \exp\left(-\pi\lambda_Y r^2\right) r \mathrm{dr}, \end{aligned} \tag{8}$$

where $\mathcal{A}(\cdot)$ is the auxiliary function given in terms of trigonometric functions and integrals,

$$\mathcal{A}(x) = \mathrm{Ci(x)}\sin(\mathrm{x}) + \left[\frac{\pi}{2} - \mathrm{Si(x)}\right]\cos(\mathrm{x}),$$

[3] Φ_X is a PPP with density λ_X outside $\mathcal{V}_{Y_0}$, and not a PPP inside $\mathcal{V}_{Y_0}$ because it has a single point at X_0 in $\mathcal{V}_{Y_0}$.

with

$$\mathrm{Ci(x)} = -\int_{\mathrm{x}}^{\infty} \frac{\cos \mathrm{t}}{\mathrm{t}} \mathrm{dt} \text{ and } \mathrm{Si(x)} = \int_{0}^{\mathrm{x}} \frac{\sin \mathrm{t}}{\mathrm{t}} \mathrm{dt}.$$

Proof: The proof is provided in Appendix B.

Note that the capture probability in (6) and (8) does not depend on P_X, since all nodes transmit with the same power and therefore both signal and interference power scale linearly with P_X. The right-hand side of (8) can be calculated numerically by a Riemann sum over r, or by a Monte-Carlo simulation of the Rayleigh random variable with parameter $(2\pi\lambda_Y)^{-1/2}$.

The derivations so far have assumed that the interfering transmitters are distributed as a homogeneous PPP. Although Φ_D and Φ_R are homogeneous PPPs, the scheduling of devices by the relays and relays by the APs ensures that no more than a single device (relay) can be active at a time in an association region of a relay (an AP). Therefore, the resulting spatial processes of simultaneously transmitting devices and relays, i.e., Φ_D^a of density $\lambda_D\delta_D$ and Φ_R^a of density $\lambda_R\delta_R$, have at most one point in each Poisson Voronoi region. Such a spatial distribution is known as Poisson Voronoi perturbed lattice or user point process (UPP) and the interference distribution resulting from Φ_D^a and Φ_R^a are intractable. In [32], the pair correlation function of UPP has been accurately characterized to approximate UPP to Ginibre Point Process or PPP depending on the cell vacancy rate. In particular, in the case where the Poisson Voronoi cells are heavily loaded with users – with the extreme case being UPP of type 1, implying exactly one user per cell – the UPP demonstrates pair correlation function similar to that of the Ginibre Point Process. On the other hand, if the Poisson Voronoi cells are lightly loaded with users the user process is called UPP of type II, and the PPP approximation is more accurate.

In our model of an IoT network, the density of transmitting devices $\lambda_D\delta_D$ has to be considerably smaller than the density of relays λ_R, and the density of transmitting relays $\lambda_R\delta_R$ has to be considerably smaller than the density of receiving AP density λ_A to ensure a reasonable end-to-end success probability. For example, as will be shown in Section V, assuming a 1-to-3 ratio of user containing cells to empty cells, i.e., $\lambda_D\delta_D \approx 0.25\lambda_R$ and $\lambda_R\delta_R \approx 0.25\lambda_A$ yields an end-to-end success probability of only 0.46. For higher success probability values, the ratio of empty cells should be even larger. Therefore, in line with the idea that UPP of type II can be well approximated to a PPP when most Poisson Voronoi cells are empty [32], replacing the UPP of interfering devices (relays) outside the association region of the typical relay (AP) with a PPP of density $\lambda_D\delta_D$ ($\lambda_R\delta_R$) provides a good approximation to the actual interference from Φ_D^a (Φ_R^a). The analysis becomes intractable without this approximation and similar approximations were also used in [33], [22], [34].

Approximating the interfering device process with a PPP of density $\lambda_D\delta_D$ outside the association region of the typical relay, we can use Theorem 1 to express the interference distribution and the outage probability for device-to-relay link as

$$\mathcal{L}_{I_{D\to R}}(s) = \exp\left\{-\pi\lambda_D p_D \mathbb{E}_\rho\left[\rho^2 C_\alpha\left(sP_D\rho^{-\alpha}\right)\right]\right\}, \quad (9)$$

where ρ is Rayleigh distributed with parameter $(2\pi\lambda_R)^{-1/2}$. Then, the outage probability for the device-to-relay link is

$$\epsilon_{D\to R} = 1 - \mathcal{C}(\lambda_D\delta_D, \lambda_R, \eta, \alpha), \quad (10)$$

with $\mathcal{C}(.)$ given in Theorem 1 for general α, and in Corollary 1 for $\alpha = 4$. Note that we use equality sign ($=$) rather than approximately equal sign ($\approx$) to indicate the approximation due to the modeling of UPP of type II as a PPP, in order to reserve the approximately equal sign for other approximations that we utilize in the upcoming sections. The PPP approximation has been thoroughly verified in the simulations as well as in other papers, e.g., [22], [35].

Similarly, the interfering relay process can be approximated with a PPP of density $\lambda_R\delta_R$ outside the association region of the typical AP. Hence, we can use Theorem 1 to express the interference distribution and the outage probability for relay-to-AP link as

$$\mathcal{L}_{I_{R\to A}}(s) = \exp\left\{-\pi\lambda_R\delta_R \mathbb{E}_\rho\left[\rho^2 C_\alpha\left(sP_R\rho^{-\alpha}\right)\right]\right\}, \quad (11)$$

where ρ is Rayleigh distributed with parameter $(2\pi\lambda_A)^{-1/2}$, and

$$\epsilon_{R\to A} = 1 - \mathcal{C}(\lambda_R\delta_R, \lambda_A, \eta, \alpha). \quad (12)$$

The accuracy of (10) and (12) for the outage probability are verified through Monte-Carlo simulations in Section V.

B. Security Links: Device-to-Sentinel and Relay-to-Sentinel

It was stated in the previous subsection that the locations of transmitting devices and relays form UPPs of type II whose Probability Generating Functional (PGFL) is intractable, and approximating the UPP of type II with a PPP of equivalent density can provide a good approximation. We resort to a similar PPP approximation to calculate the interference received at a sentinel node. In particular, we approximate the spatial distributions of actively transmitting devices and relays with homogeneous PPPs of densities $\lambda_D\delta_D$ and $\lambda_R\delta_R$, respectively. Since there is no rule describing the positions of transmitting relays and devices relative to the sentinels, the received interference distributions at the typical sentinel is straightforward. The Laplace transform of the interference from homogeneous PPP distributed transmitters of density λ_X with Rayleigh fading assumption is known to be (from [36], Eq. (8)),

$$\mathcal{L}_I(s) = \exp\left(-\pi\lambda_X P_X^{\frac{2}{\alpha}} s^{\frac{2}{\alpha}} K_\alpha\right), \quad (13)$$

where $K_\alpha = 2\pi/[\alpha\sin(2\pi/\alpha)]$.

Likewise, the received interference distribution at the typical sentinel, when decoding device and relay packets respectively would be,

$$\begin{aligned}\mathcal{L}_{I_{D\to S}}(s) &= \exp\left(-\pi\lambda_D\delta_D P_D^{\frac{2}{\alpha}} s^{\frac{2}{\alpha}} K_\alpha\right),\\ \mathcal{L}_{I_{R\to S}}(s) &= \exp\left(-\pi\lambda_R\delta_R P_R^{\frac{2}{\alpha}} s^{\frac{2}{\alpha}} K_\alpha\right).\end{aligned} \quad (14)$$

B.1 Isolated Detection

In the following, we calculate the capture probability for relay-to-sentinel links by conditioning on the distance between the typical sentinel and its associated relay, i.e., $\|S_0 - R_0\|$, according to the isolated detection scheme. Since the association between relays and sentinels is such that each relay is linked to its nearest sentinel, the distance between the typical sentinel at $S_0 \in \Phi_S$ and its associated relay at $R_0 \in \Phi_R^a \cap \mathcal{V}_{S_0}$ has a Rayleigh distribution with parameter $(2\pi\lambda_S)^{-1/2}$. Then, the probability that the typical sentinel captures the packet transmitted by its tagged relay at $R_0 \in \Phi_R^a \cap \mathcal{V}_{S_0}$ can be calculated by integrating the conditional capture probability over the distance distribution of $\|S_0 - R_0\|$,

$$
\begin{aligned}
&1 - \epsilon_{R\to S}^{(i)} \\
&= \int_0^\infty \Pr\left(\frac{P_R h_{S_0,R_0}\|S_0 - R_0\|^{-\alpha}}{I_{R\to S}} \geq \eta \mid \|S_0 - R_0\| = r\right) \\
&\qquad \times f_{\|S_0-R_0\|}(r)\mathrm{d}r \\
&\overset{(a)}{=} 2\pi\lambda_S \int_0^\infty \mathbb{E}\left\{\exp\left[-\frac{\eta r^\alpha}{P_R} I_{R\to S}\right]\right\} \exp\left(-\pi\lambda_S r^2\right) r\mathrm{d}r \\
&\overset{(b)}{=} 2\pi\lambda_S \int_0^\infty \exp\left(-\pi\lambda_R \delta_R \eta^{\frac{2}{\alpha}} K_\alpha r^2\right) \exp\left(-\pi\lambda_S r^2\right) r\mathrm{d}r \\
&\overset{(c)}{=} \left(\frac{\lambda_R \delta_R}{\lambda_S} \eta^{\frac{2}{\alpha}} K_\alpha + 1\right)^{-1}, \qquad (15)
\end{aligned}
$$

where (a) follows from the complementary cumulative distribution function of the exponential random variable h_{S_0,R_0}, (b) from substituting the Laplace transform $\mathcal{L}_{I_{R\to S}}(s)$ from (14), and (c) from evaluating the integral by the change of variables $v \leftarrow r^2$. This result is reasonable as an increased transmitting relay density would result in higher interference, reducing the capture probability; whereas an increased sentinel density stochastically reduces the nearest sentinel distance, thus improving the capture probability.

We now proceed to analyze the capture probability for device-to-sentinel links, by analyzing the distance distribution between a sentinel and its associated device. As stated in Section II, each device is monitored by the same sentinels with its receiving relay, in order for this sentinel to overhear and compare the device's and relay's transmission of a particular data packet. Let us denote the distances between the associated pairs of relay/sentinel and device/relay nodes by r_{RS}, r_{DR} respectively. Then, the distance between the associated pair of device/sentinel nodes can be expressed as

$$
r_{\mathrm{DS}} = \left(r_{\mathrm{RS}}^2 + r_{\mathrm{DR}}^2 - 2r_{\mathrm{RS}} r_{\mathrm{DR}} \cos\theta\right)^{\frac{1}{2}}, \qquad (16)
$$

where θ is as shown in Fig. 2. Considering that r_{RS} and r_{DR} are Rayleigh distributed (nearest Poisson point distribution) with parameters $(2\pi\lambda_S)^{-1/2}$ and $(2\pi\lambda_R)^{-1/2}$ respectively, and the PDF of θ, $f(\theta) = 1/(2\pi)$ in $[0, 2\pi)$, the distribution of r_{DS} can only be expressed in terms of iterated integrals. For tractability, we conjecture that the distribution of r_{DS} is similar to a Rayleigh distribution with an appropriate parameter. If r_{DS} is assumed to be Rayleigh distributed, r_{DS}^2 is exponentially distributed. We choose the mean of r_{DS}^2 as

$$
\begin{aligned}
\mathbb{E}\left[r_{\mathrm{DS}}^2\right] &= \mathbb{E}\left[r_{\mathrm{RS}}^2 + r_{\mathrm{DR}}^2 - 2r_{\mathrm{RS}} r_{\mathrm{DR}} \cos\theta\right] \\
&= \frac{1}{\pi\lambda_S} + \frac{1}{\pi\lambda_R} = \frac{\lambda_S + \lambda_R}{\pi\lambda_S\lambda_R}, \qquad (17)
\end{aligned}
$$

which follows from the fact that r_{RS}^2 and r_{DR}^2 are exponential random variables with parameters $1/(\pi\lambda_S)$ and $1/(\pi\lambda_R)$ and θ is uniformly distributed in $[0, 2\pi)$. Thus,

$$
f_{r_{\mathrm{DS}}^2}(t) \approx \frac{\pi\lambda_S\lambda_R}{\lambda_S + \lambda_R} \exp\left(-\frac{\pi\lambda_S\lambda_R}{\lambda_S + \lambda_R} t\right) \qquad (18)
$$

is the approximate distribution of r_{DS}^2. The accuracy of this approximation is verified in Fig. 3 where the cumulative distribution functions of the approximate r_{DS}^2 and Monte-Carlo calculated distance square between the associated device-sentinel pairs are compared.

Then, the probability that the typical sentinel captures the packet transmitted by its associated device can be calculated by integrating the conditional capture probability over the distribu-

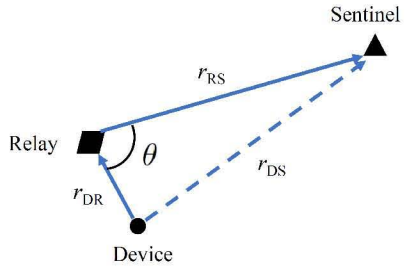

Fig. 2. An illustration of distances between the associated devices, relays and sentinels.

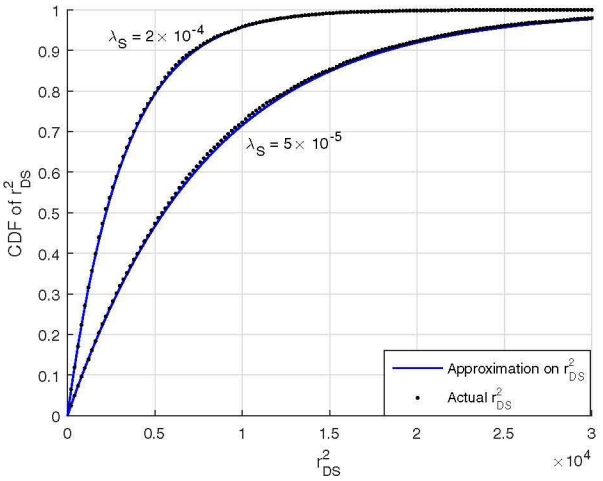

Fig. 3. Comparison of the cumulative distribution functions of approximate r_{DS}^2 (distribution given as in (18)) and Monte-Carlo calculated r_{DS}^2. $\lambda_D = 10^{-3}$, $\lambda_R = 2 \times 10^{-4}$. The comparison is presented for two different sentinel densities as shown on the figure.

tion of $r_{\text{DS}}^2 = \|S_0 - R_0\|^2$ given in (18),

$$\begin{aligned}
&1-\epsilon_{D\to S}^{(i)}\\
&\approx \int_0^\infty \Pr\left(\frac{P_D h_{S_0,D_0}\|S_0-D_0\|^{-\alpha}}{I_{D\to S}} \geq \eta \mid \|S_0-D_0\|^2 = t\right)\\
&\qquad \times f_{r_{\text{DS}}^2}(t)\text{dt}\\
&= \frac{\pi\lambda_S\lambda_R}{\lambda_S+\lambda_R}\int_0^\infty \exp\left(-\pi\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha t\right)\exp\left(-\frac{\pi\lambda_S\lambda_R}{\lambda_S+\lambda_R}t\right)\text{dt}\\
&= \left[\frac{\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha(\lambda_S+\lambda_R)}{\lambda_S\lambda_R}+1\right]^{-1}. \qquad (19)
\end{aligned}$$

B.2 Co-operative Detection

In co-operative detection, the packet transmitted by the typical relay at R_0 cannot be detected if none of the sentinels in Φ_S captures the packet transmitted by this relay. Specifically,

$$\epsilon_{R\to S}^{(c)} = \prod_{S_i\in\Phi_s} \epsilon_{R_0\to S_i}, \qquad (20)$$

in which $\epsilon_{R_0\to S_i}$ denotes the miss-detection probability of the transmission from the typical relay to sentinel at S_i, i.e.,

$$\epsilon_{R_0\to S_i} = 1-\Pr\left(\frac{P_R h_{S_i,R_0}\|S_i-R_0\|^{-\alpha}}{I_{R\to S_i}} \geq \eta\right), \qquad (21)$$

$\forall S_i \in \Phi_S$ similar to (1). The right-hand-side of (20) can be evaluated by using PGFLs,

$$\begin{aligned}
&1-\epsilon_{R\to S}^{(c)}\\
&= 1-\mathbb{E}\prod_{S_i\in\Phi_s}\left[1-\Pr\left(\frac{P_R h_{S_i,R_0}\|S_i-R_0\|^{-\alpha}}{I_{R\to S_i}}\geq\eta\right)\right]\\
&\overset{(a)}{=} 1-\mathbb{E}\prod_{S_i\in\Phi_s}\left[1-\mathbb{E}\left\{\exp\left(-\frac{\eta\|S_i-R_0\|^\alpha}{P_R}I_{R\to S_i}\right)\right\}\right]\\
&\overset{(b)}{=} 1-\mathbb{E}\prod_{S_i\in\Phi_s}\left[1-\exp\left(-\pi\lambda_R\delta_R\eta^{\frac{2}{\alpha}}K_\alpha\|S_i-R_0\|\right)\right]\\
&\overset{(c)}{=} 1-\exp\left[-2\pi\lambda_S\int_0^\infty \exp\left(-\pi\lambda_R\delta_R\eta^{\frac{2}{\alpha}}K_\alpha r^2\right)r\text{dr}\right]\\
&= 1-\exp\left(-\frac{\lambda_S}{\lambda_R\delta_R\eta^{\frac{2}{\alpha}}K_\alpha}\right), \qquad (22)
\end{aligned}$$

where (a) follows from the complementary cumulative distribution function of h_{S_i,R_0}, (b) from substituting the Laplace transform of $I_{R\to S_i}$ at $s=\eta\|S_i-R_0\|^\alpha/P_R$ using (14), (c) from the fact that the expectation of a product over a point process is a PGFL, thus using the PGFL of a PPP from (A.3) in [37] with the intensity function $\Lambda(r) = 2\pi r\lambda_S$, and the last step from evaluating the integral by the change of variables $v \leftarrow r^2$.

Similarly, the packet transmitted by the typical device at D_0 cannot be detected if none of the sentinels in Φ_S captures the packet transmitted by this device,

$$\epsilon_{D\to S}^{(c)} = \prod_{S_i\in\Phi_s}\epsilon_{D_0\to S_i}. \qquad (23)$$

Going through the same steps as in (22), we have the capture probability of device packets as

$$1-\epsilon_{D\to S}^{(c)} = 1-\exp\left(-\frac{\lambda_S}{\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha}\right). \qquad (24)$$

IV. PROBLEM FORMULATION and OPTIMIZATION

With the expressions derived above, it is possible to solve problems such as finding the minimal sentinel density to ensure a certain detection probability, given other network parameters. In the following, we formulate and solve Problem 1 for both isolated detection and co-operative detection schemes.

Problem 1.

$$\begin{aligned}
&\min_{\lambda_S}\ \lambda_S\\
&\text{s.t.,}\ (1-\epsilon_{R\to S})(1-\epsilon_{D\to S}) \geq T\\
&\qquad \lambda_S \geq 0.
\end{aligned}$$

To solve Problem 1, the expressions for $(1-\epsilon_{R\to S})$ and $(1-\epsilon_{D\to S})$ can be substituted from (15) and (19) for isolated detection and from (22) and (24) for co-operative detection.

A. Solution for Isolated Detection

From (15) and (19), one can note that $(1-\epsilon_{R\to S}^{(i)})$ and $(1-\epsilon_{D\to S}^{(i)})$ are both increasing functions of λ_S. In other words, the probability that the typical sentinel captures both the tagged device and relay versions of the packet increases with increasing sentinel density. Therefore, λ_S^* is attained when the first inequality constraint is satisfied with equality,

$$\begin{aligned}
T &= (1-\epsilon_{R\to S}^{(i)})(1-\epsilon_{D\to S}^{(i)})\\
&= \left(\frac{\lambda_R\delta_R}{\lambda_S^*}\eta^{\frac{2}{\alpha}}K_\alpha+1\right)^{-1}\left[\frac{\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha(\lambda_S^*+\lambda_R)}{\lambda_S^*\lambda_R}+1\right]^{-1}. \qquad (25)
\end{aligned}$$

$$\begin{aligned}
\lambda_S^* = &-T\lambda_R\Big\{\eta^{\frac{2}{\alpha}}K_\alpha\Big[(\lambda_D^2\delta_D^2+\lambda_R^2\delta_R^2+4\lambda_D\delta_D\lambda_R\delta_R/T\\
&-2\lambda_D^2\delta_D^2\delta_R\eta^{\frac{2}{\alpha}}K_\alpha-2\lambda_D\delta_D\lambda_R\delta_R\\
&+\lambda_D^2\delta_D^2\delta_R^2\eta^{\frac{4}{\alpha}}K_\alpha^2+2\lambda_D\delta_D\lambda_R\delta_R^2\eta^{\frac{2}{\alpha}}K_\alpha)^{\frac{1}{2}}\\
&+\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha+\lambda_R\delta_R\eta^{\frac{2}{\alpha}}K_\alpha+\lambda_D\delta_D\delta_R\eta^{\frac{4}{\alpha}}K_\alpha^2\Big]\Big\}\\
&/\left[2(T\lambda_R-\lambda_R+T\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha)\right]. \qquad (26)
\end{aligned}$$

B. Solution for Co-operative Detection

Similarly $(1-\epsilon_{R\to S}^{(c)})$ from (22) and $(1-\epsilon_{D\to S}^{(c)})$ from (24) are increasing functions of λ_S. Thus, λ_S^* is minimized when the first inequality constraint is satisfied with equality. An implicit solution exists for λ_S^*,

$$\begin{aligned}
&(1-\epsilon_{R\to S}^{(c)})(1-\epsilon_{D\to S}^{(c)}) = T\\
&\left[1-\exp\left(-\frac{\lambda_S^*}{\lambda_R\delta_R\eta^{\frac{2}{\alpha}}K_\alpha}\right)\right]\left[1-\exp\left(-\frac{\lambda_S^*}{\lambda_D\delta_D\eta^{\frac{2}{\alpha}}K_\alpha}\right)\right]\\
&\qquad = T. \qquad (27)
\end{aligned}$$

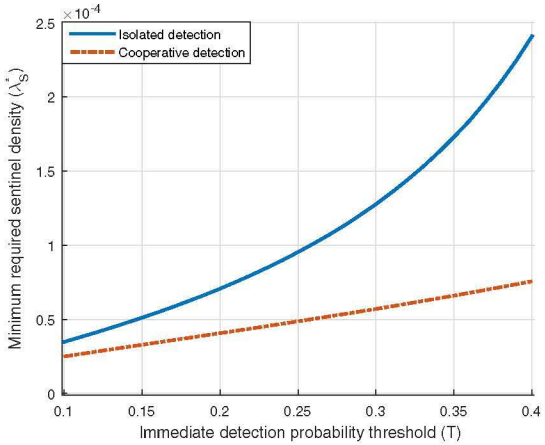

Fig. 4. Minimum sentinel density required to achieve desired immediate detection probability. The parameters are $\lambda_D = 10^{-3}$, $\lambda_R = 2 \times 10^{-4}$, $\delta_D = 0.05$, $\delta_R = 0.05$, $\eta = 3$, $\alpha = 4$.

Table 1. Parameters used in the simulations.

Parameter	Value
λ_D	10^{-3} nodes/m^2
λ_R	2×10^{-4} nodes/m^2
λ_s	10^{-4} nodes/m^2
λ_B	4×10^{-5} nodes/m^2
δ_D	0.05
δ_R	0.05
η	3
α	4

Based on the solutions of (26) and (27), the minimum required sentinel density λ_S^* to achieve a certain immediate detection probability is shown in Fig. 4. The isolated detection model is much more sensitive to the detection threshold, i.e., it requires significantly denser sentinel deployment to achieve a given detection probability.

V. SIMULATIONS and DISCUSSION

A. Numerical Results

In this section, Monte-Carlo simulations are presented to confirm the accuracy of the analytical results and to obtain insights on how system parameters affect the detection performance and end-to-end success rate of IoT transmissions. The parameters in Table 1 are used for simulations unless otherwise indicated in the plots.

In Fig. 5, the probability that a packet transmitted by devices or relays is captured by sentinels is plotted against the sentinel density. In general, the analytical plots follow the same trend as the Monte-Carlo plots. The limited discrepancy between the analytical and simulation plots of the isolated detection scheme is due to the PPP assumption of interfering nodes, and also due to the approximation (conjectured in (18)) on the distance distribution between a device and its associated sentinel.

Fig. 6 shows the detection probability of an attack, in comparison with the end-to-end success probability of IoT packets, plotted over the density of transmitting devices. As $\lambda_D \delta_D$

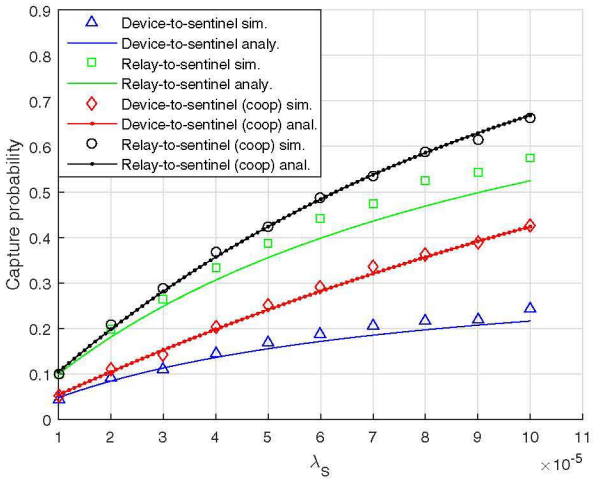

Fig. 5. Capture probability of sentinels over sentinel density, under isolated and cooperative detection models.

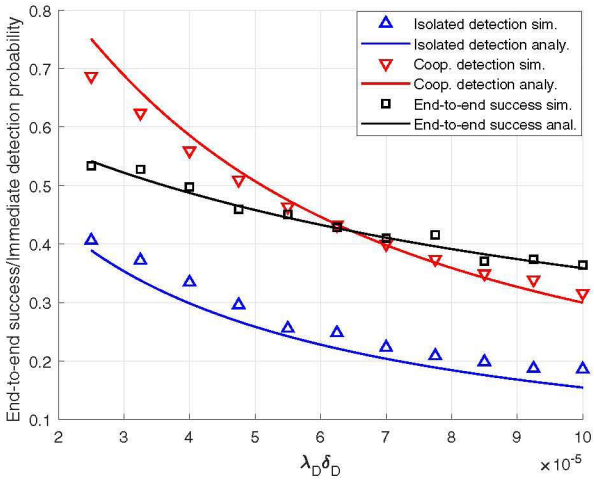

Fig. 6. The comparison of end-to-end transmission success probability (squares) and immediate detection probability of sentinels (triangles) over transmitting device density.

increases, the interference in device-to-relay and device-to-sentinel links also increases, resulting in a lower capture probability in these links. Therefore, all three plots are decaying as transmitting device density is increasing. The rate of decay in sentinel detection probability is higher than that of end-to-end success probability, suggesting that the detection model is more sensitive to the interference level when capturing device packets.

Figs. 7 and 8 illustrate the detection probability of an attack, in comparison with the end-to-end success probability of IoT packets, plotted over the density of relays and ratio of transmitting relays respectively. Note that as relay density increases, typical device-to-relay distance decreases, resulting in a better capture probability for device-to relay links. On the other hand, increasing relay density increases the interference caused by the relays, reducing the capture probability at relay-to-AP links. The former effect is dominant up until $\lambda_R \approx 2 \times 10^{-4}$, whereas the latter dominates for larger λ_R as can be seen from

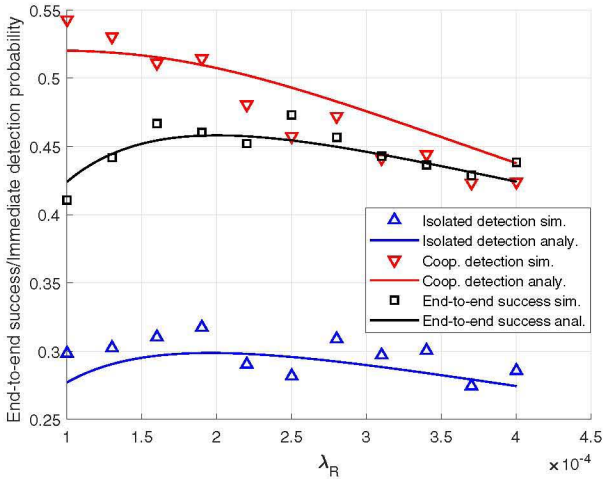

Fig. 7. The comparison of end-to-end transmission success probability (squares) and immediate detection probability of sentinels (triangles) over relay density.

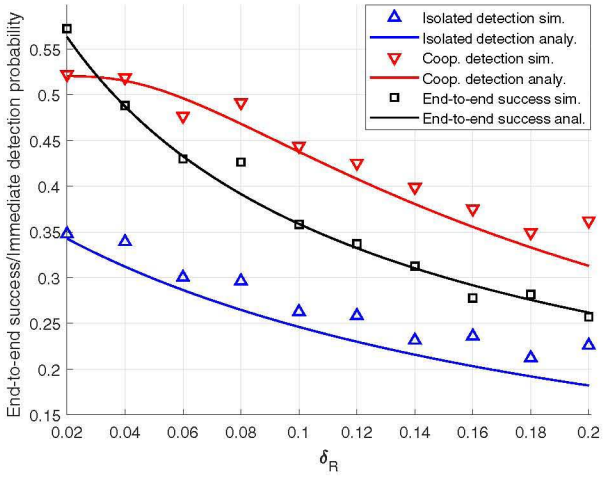

Fig. 8. The comparison of end-to-end transmission success probability (squares) and immediate detection probability of sentinels (triangles) over the ratio of transmitting relays.

the end-to-end success probability plot (black squares). Both the attack detection probability and end-to-end success probability consistently decrease with the ratio of transmitting relays due to increased interference. At low relay densities, the analytical plot of the isolated detection scheme is less accurate due to the approximation in (18).

B. Discussion

The foremost finding of this paper is that using passive sentinel nodes – even when they are much less in number than the relay nodes – to monitor data traffic in an IoT relay network is feasible from the communication theory perspective. This finding can be observed from Figs. 5–8, where $\lambda_S < \lambda_R$ leads to similar performance between the end-to-end success probability of the network and the attack detection probability of sentinels. It should also be noted that these Figures display the immediate detection probability of an attack performed on a single packet. As multiple packets are observed by the sentinel, the detection probability increases dramatically.

The sentinel-based detection is scalable because the task of each sentinel is simply to compare the transmitted MAC payload from a device in its vicinity with the corresponding payload forwarded by the relay. Even in co-operative detection, the sentinels only need to exchange certain messages locally, thus the increasing network area does not translate into a larger number of exchanged messages between the sentinels. The sentinel-based detection can also be considered in a multi-hop setting wherein sentinels compare the MAC payload transmitted by nodes with the corresponding payload forwarded by the respective next-hop-nodes in their vicinity. In this manner, the attack detection for each hop is an independent task, the probability of which is calculated in this paper.

Our sentinel approach has several advantages over other network intrusion detection systems and techniques [10]–[12]. Firstly, the proposed method does not require any change in the existing protocols or deployed devices but rather introduces a new set of sentinel nodes. Since the intrusion detection is performed only at the external sentinel devices, the IoT network is not burdened with computational load or signaling overhead unlike the prior work.

Secondly, the security of the users would be compromised if the intrusion detection system itself is compromised. It can be safely argued that the passive sentinel devices can be designed with the latest security technologies (e.g., Trusted Execution Environment), therefore, they would be less prone to attacks than any other wireless device in an IoT network. Privacy measures such as imposing hardware limitations on the transmit interfaces of the sentinel devices can be considered to protect the privacy of the IoT network. Therefore, integrity checking by sentinels would be a more secure approach than offloading such a critical task to the network whose integrity is questionable in the first place. On the other hand, we acknowledge that there will be a hardware cost (and bandwidth cost for co-operative detection) of deploying sentinels. Yet, the costs will be limited because very good attack detection performance can be achieved with $\lambda_S < \lambda_R$.

Thirdly, the false alarm rate in our sentinel based detection scheme is negligible as it occurs only in the unlikely scenario where the packet CRC fails to detect errors, even though the decoded packet is in error. Further, the detection scheme operates at the MAC layer and therefore remains effective even in scenarios where different wireless links may employ distinct modulation and coding schemes at the physical layer.

Finally, the other methods commonly relied on known channel parameters in their analysis which is unrealistic in a large IoT network. Through the use of stochastic geometry, we have demonstrated the feasibility of our sentinel-based method from a communication theoretical perspective. It should be noted however that, the use of stochastic geometry also has a downside. It only provides system-level insights (e.g., detection performance as a function of node densities) for an *average* network rather than suggesting precise refinements to a specific network. Hence, the fine-tuning of other useful parameters (e.g., finding exact sentinel locations, varying sentinel density based on the IoT network load) are not studied in this paper and will be in-

vestigated in future work.

VI. CONCLUSION

In this paper, we have proposed sentinel based attack detection schemes to identify malicious relays that alter, drop or craft data packets in an IoT network. The proposed schemes are well suited to resource-constrained IoT networks and can supplement higher-layer security mechanisms. We have applied a stochastic geometry approach to interference modeling, and hence optimized the density of sentinel nodes for given densities of relay and IoT devices, as well as the desired attack detection probability. Co-operative detection performance is shown to be significantly better than that of isolated detection because the packet modifications can be detected in the co-operative scheme when the device and relay versions of the same packet are captured by different sentinels. On the other hand, isolated detection requires no communication among sentinels, except for the initial association region setup. Minimum sentinel density to achieve a certain attack detection performance was calculated for both schemes. It has been shown that the required sentinel density (especially in co-operative detection) can be much smaller than the relay density to achieve a detection probability approximately equal to the end-to-end success probability of the IoT network. This outcome, combined with the fact that sentinels do not add computational burden to the IoT network, confirms sentinels as viable solutions for preserving data integrity in IoT relay networks.

APPENDIX A
PROOF OF THEOREM 1

The intensity function of the interfering nodes is λ_X outside $\mathcal{V}_{Y_0}$. Transforming into polar coordinates, we have intensity function of $\Lambda(r) = 2\pi r\lambda_X$ defined outside $\mathcal{V}_{Y_0}$, with r denoting the distance from the origin (or Y_0). Let ρ_X, $\forall X \in \Phi_X$ denote the distances between the interfering nodes and their intended receivers. Therefore, ρ_X's are i.i.d with a nearest Poisson point distribution, i.e., Rayleigh distribution,

$$f_\rho(\rho) = 2\pi\lambda_Y \rho \exp\left(-\pi\lambda_Y \rho^2\right). \tag{28}$$

The interfering nodes are outside $\mathcal{V}_{Y_0}$ if and only if they are farther from the origin than they are to their associated receivers at $Y_i \in \Phi_Y$ as specified by association rule in (3). Specifically, $\|X\| > \rho_X$, $\forall X \in \Phi_X \backslash \{X_0\}$. Hence, the intensity function of the interfering nodes defined in $\mathbb{R}^2$ is $\Lambda(r) = 2\pi r\lambda_X \mathbb{1}(r > \rho_X)$, where $\mathbb{1}(\cdot)$ is the indicator function. Using this intensity function, the Laplace transform of the interference distribution in (4) can be evaluated as follows.

$$\begin{aligned}
\mathcal{L}_{I_{Y_0}}(s) &= \mathbb{E}\left[\prod_{X\in\Phi_X\backslash\mathcal{V}_{Y_0}} \exp\left(-sP_X h_{Y_0,X}\|X\|^{-\alpha}\right)\right] \\
&\overset{(a)}{=} \mathbb{E}\left[\prod_{X\in\Phi_X\backslash\mathcal{V}_{Y_0}} \frac{1}{1+sP_X\|X\|^{-\alpha}}\right] \\
&\overset{(b)}{=} \exp\left\{-2\pi\lambda_X \mathbb{E}_\rho\left[\int_{r>\rho} \frac{r\mathrm{dr}}{1+s^{-1}P_X^{-1}r^\alpha}\right]\right\} \\
&\overset{(c)}{=} \exp\left\{-\pi\lambda_X \mathbb{E}_\rho\left[\rho^2 \int_1^\infty \frac{\mathrm{dt}}{1+s^{-1}P_X^{-1}\rho^\alpha t^{\alpha/2}}\right]\right\} \\
&= \exp\left\{-\pi\lambda_X \mathbb{E}_\rho\left[\rho^2 C_\alpha\left(sP_X\rho^{-\alpha}\right)\right]\right\},
\end{aligned} \tag{29}$$

where (a) follows from the i.i.d nature of $\{h_{Y_0,X}\}$s and their Moment Generating Function (MGF), (b) from using the Probability Generating Functional (PGFL) of the inhomogeneous PPP $\Phi_X\backslash\mathcal{V}_{Y_0}$ with intensity function $\Lambda(r) = 2\pi rq\lambda_X \mathbb{1}(\mathbb{r} > \rho_{\mathbb{X}})$ ((A.3) in [37]) and (c) from the change of variables $t \leftarrow r^2/\rho^2$.

From (1), the capture probability $1-\epsilon_{X\to Y}$ can be calculated by de-conditioning on the typical transmitter/receiver distance $\|Y_0 - X_0\| = r$,

$$\begin{aligned}
&1-\epsilon_{X\to Y} \\
&= \int_0^\infty \Pr\left(\frac{P_X h_{Y_0,X_0}\|Y_0-X_0\|^{-\alpha}}{I_{Y_0}} \geq \eta \mid \|Y_0-X_0\| = r\right) \\
&\qquad \times f_{\|Y_0-X_0\|}(r)\mathrm{dr} \\
&\overset{(a)}{=} 2\pi\lambda_Y \int_0^\infty \mathbb{E}\left[\exp\left(-\frac{\eta r^\alpha}{P_X} I_{Y_0}\right)\right] \exp\left(-\pi\lambda_Y r^2\right) r\mathrm{dr} \\
&\overset{(b)}{=} 2\pi\lambda_Y \int_0^\infty \mathcal{L}_{I_{Y_0}}\left(\frac{\eta r^\alpha}{P_X}\right) \exp\left(-\pi\lambda_Y r^2\right) r\mathrm{dr},
\end{aligned} \tag{30}$$

where (a) follows from the complementary cumulative distribution function of the exponential random variable h_{Y_0,X_0} and by substituting the nearest Poisson point distribution $f_{\|Y_0-X_0\|}(r) = 2\pi\lambda_Y e^{-\pi\lambda_Y r^2}$, and (b) is because the expression inside the expected value operator is in the form of the Laplace transform of the distribution of I_{Y_0} evaluated at $s = \eta r^\alpha/P_X$.

APPENDIX B
PROOF OF COROLLARY 1

We first show that,

$$\begin{aligned}
&\mathbb{E}_\rho\left[\rho^2 C_4(w^2\rho^{-4})\right] \\
&= 2\pi\lambda\int_0^\infty\int_1^\infty \frac{\mathrm{dt}}{1+w^{-2}\rho^4 t^2}\exp(-\pi\lambda\rho^2)\rho^3\mathrm{d}\rho \\
&\overset{(a)}{=} \pi\lambda w^2\int_0^\infty\int_1^\infty \frac{\mathrm{dt}}{1+r^2t^2}\exp(-\pi\lambda T r) r\mathrm{dr} \\
&\overset{(b)}{=} \pi\lambda w^2\int_0^\infty \cot^{-1}(r)\exp(-\pi\lambda w r)\mathrm{dr} \\
&\overset{(c)}{=} w\left[\frac{\pi}{2} - \int_0^\infty \frac{\exp(-\pi\lambda w r)}{1+r^2}\mathrm{dr}\right] \\
&= w\left[\frac{\pi}{2} - \mathcal{A}(\pi\lambda w)\right],
\end{aligned} \tag{31}$$

where (a) follows from the change of variables $r \leftarrow \rho^2/w$, (b) from solving the inner integral by noting $\mathrm{d}(\tan^{-1}(\mathrm{rt}))/\mathrm{dt} = \mathrm{r}/(1+\mathrm{r}^2\mathrm{t}^2)$, (c) from integration by parts with $u = \cot^{-1}(r)$, $\mathrm{dv} = \exp(-\pi\lambda\mathrm{wr})\mathrm{dr}$, and the last step from expressing the integral in terms of the auxiliary function,

$$\mathcal{A}(x) = \int_0^\infty \frac{\exp(-xr)}{1+r^2}\mathrm{dr} = \mathrm{Ci(x)}\sin(\mathrm{x}) + \left[\frac{\pi}{2} - \mathrm{Si(x)}\right]\cos(\mathrm{x}).$$

Then, the above result with $w = \sqrt{sP_X}$ can be used in (5), to replace $\mathbb{E}_\rho\left[\rho^2 C_\alpha(sP_X\rho^{-\alpha})\right]$ with $\sqrt{sP_X}\left(\frac{\pi}{2} - \mathcal{A}(\pi\lambda_Y\sqrt{sP_X})\right)$,

$$\mathcal{L}_{I_{Y_0}}(s) = \exp\left\{-\pi\lambda_X\sqrt{sP_X}\left[\frac{\pi}{2} - \mathcal{A}(\pi\lambda_Y\sqrt{sP_X})\right]\right\}. \tag{32}$$

Finally, (32) can be integrated over the distance distribution $f_{\|Y_0 - X_0\|}(r) = 2\pi\lambda_Y e^{-\pi\lambda_Y r^2}$ for $r \geq 0$ to obtain the capture probability in (8).

REFERENCES

[1] S. Zhang, J. Peng, K. Huang, X. Xu, and Z. Zhong, "Physical layer security in iot: A spatial-temporal perspective," in *Proc. IEEE WCSP*, Oct. 2017, pp. 1–6.

[2] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[3] A. Tandon, T. J. Lim, and U. Tefek, "Sentinel based malicious relay detection scheme for wireless IoT networks," in *Proc. IEEE GLOBECOM*, Dec. 2018, pp. 1–6.

[4] A. Tandon, T. J. Lim, and U. Tefek, "Sentinel based malicious relay detection in wireless IoT networks," *J. Commun. Netw.*, vol. 21, no. 5, pp. 458–468, Oct. 2019.

[5] C. Jia and T. J. Lim, "Detecting cluster head attacks in heterogeneous wireless sensor networks," in *Proc. IEEE VTC*, June 2017, pp. 1–6.

[6] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3718–3731, May 2016.

[7] S. W. Kim, "Physical integrity check in cooperative relay communications," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6401–6413, Nov. 2015.

[8] X. Liu, Y. Guan, and S. W. Kim, "Bayesian test for detecting false data injection in wireless relay networks," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 380–383, Feb. 2018.

[9] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," in *Proc. IEEE ICICS*, Dec. 2009, pp. 1–5.

[10] C. Pu and S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: Design, analysis, and evaluation," *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–9, 2016.

[11] D. Agarwal, R. R. Rout, and S. Ravichandra, "Detection of node-misbehavior using overhearing and autonomous agents in wireless ad-hoc networks," in *Proc. IEEE AIMoC*, Feb. 2015, pp. 152–157.

[12] T. H. Hai and E. N. Huh, "Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge," in *Proc. IEEE NCA*, July 2008, pp. 325–331.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom*, Aug. 2000, pp. 255–265.

[14] R. Cao, "Detecting arbitrary attacks using continuous secured side information in wireless networks," *IEEE Access*, vol. 5, pp. 25 927–25 945, 2017.

[15] R. Cao, T. F. Wong, T. Lv, H. Gao, and S. Yang, "Detecting byzantine attacks without clean reference," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2717–2731, Dec. 2016.

[16] T. Lv, Y. Yin, Y. Lu, S. Yang, E. Liu, and G. Clapworthy, "Physical detection of misbehavior in relay systems with unreliable channel state information," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1517–1530, July 2018.

[17] Y. J. Chun, M. O. Hasna, and A. Ghrayeb, "Modeling heterogeneous cellular networks interference using Poisson cluster processes," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2182–2195, Oct. 2015.

[18] R. W. Heath, M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using Poisson point processes," *IEEE Trans. Signal Proc.*, vol. 61, no. 16, pp. 4114–4126, Aug. 2013.

[19] S. Cho and W. Choi, "Energy-efficient repulsive cell activation for heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 5, pp. 870–882, May 2013.

[20] U. Tefek and T. J. Lim, "Full-duplex relaying in machine-type communications with a multi-antenna base station," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5804–5817, Sept. 2018.

[21] J. Guo, S. Durrani, X. Zhou, and H. Yanikomeroglu, "Massive machine type communication with data aggregation and resource scheduling," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 4012–4026, Sept. 2017.

[22] D. Malak, H. S. Dhillon, and J. G. Andrews, "Optimizing data aggregation for uplink machine-to-machine communication networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1274–1290, Mar. 2016.

[23] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

[24] X. Liu, K. Zheng, X. Liu, X. Wang, and G. Dai, "Towards secure and energy-efficient crns via embracing interference: A stochastic geometry approach," *IEEE Access*, vol. 6, pp. 36 757–36 770, 2018.

[25] Y. Cai, X. Xu, and W. Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise," *IET Commun.*, vol. 10, no. 15, pp. 1904–1913, 2016.

[26] M. A. Kishk and H. S. Dhillon, "Stochastic geometry-based comparison of secrecy enhancement techniques in d2d networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 394–397, June 2017.

[27] M. A. Kishk and H. S. Dhillon, "Coexistence of RF-powered IoT and a primary wireless network with secrecy guard zones," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1460–1473, Mar. 2018.

[28] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Select. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, June 2015.

[29] P. Huang, Y. Hao, T. Lv, J. Xing, J. Yang, and P. T. Mathiopoulos, "Secure beamforming design in relay-assisted internet of things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6453–6464, Aug. 2019.

[30] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 2, pp. 198–212, June 2007.

[31] D. Stoyan, W. S. Kendall, J. Mecke, and L. Ruschendorf, *Stochastic geometry and its applications*. Wiley New York, 1987, vol. 2.

[32] M. Haenggi, "User point processes in cellular networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 258–261, Apr. 2017.

[33] S. Singh, X. Zhang, and J. G. Andrews, "Joint rate and SINR coverage analysis for decoupled uplink-downlink biased cell associations in hetnets," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5360–5373, Oct. 2015.

[34] U. Tefek and T. J. Lim, "Relaying and radio resource partitioning for machine-type communications in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1344–1356, Feb. 2017.

[35] S. Singh, X. Zhang, and J. G. Andrews, "Joint rate and SINR coverage analysis for decoupled uplink-downlink biased cell associations in hetnets," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5360–5373, Oct. 2015.
[36] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sept. 2009.
[37] M. Haenggi and R. K. Ganti, *Interference in large wireless networks*. Now Publishers Inc, 2009.

Utku Tefek received the B.Sc. degree with high honors in Electrical and Electronics Engineering from Bilkent University, Turkey in 2013 and the Ph.D. degree from the National University of Singapore in 2017. From October 2017 to October 2018, he was a Postdoctoral Researcher at the National University of Singapore (NUS), Singapore. Since October 2018, he has been with ADSC (Advanced Digital Sciences Center), an affiliate of the University of Illinois. His research interests include the application of stochastic models to wireless networks, machine-to-machine communications and cyberphysical system security.

Anshoo Tandon received the B.E. degree in Computer Science and Engineering from Kumaun University, Nainital, India, in 1998, the M.E. degree in Signal Processing from the Indian Institute of Science, Bengaluru, India, in 2000, and the Ph.D. degree from the National University of Singapore (NUS), Singapore, in 2016. Between 2000 and 2011, he worked in different capacities in the industry towards developing efficient cellular and wireless connectivity solutions. He is currently a Research Fellow in the Department of Electrical and Computer Engineering at NUS, Singapore. His research interests include information theory, coding theory, and design of efficient communication systems.

Teng Joon (T. J.) Lim (S'92-M'95-SM'02-F'17) obtained the B.Eng. degree in Electrical Engineering with first-class honours from the National University of Singapore (NUS) in 1992, and the Ph.D. degree from the University of Cambridge in 1996. From September 1995 to November 2000, he was a Researcher at the Centre for Wireless Communications in Singapore, one of the predecessors of the Institute for Infocomm Research (I2R). From December 2000 to May 2011, he was Assistant Professor, Associate Professor, then Professor at the University of Toronto's Edward S. Rogers Sr. Department of Electrical and Computer Engineering. From June 2011 to January 2020, he was a Professor at the Electrical Computer Engineering Department of NUS, where he served as a Deputy Head from July 2014 to August 2015. From September 2015 through December 2019, he served as Vice-Dean (Graduate Programs) in the NUS Faculty of Engineering. Since January 2020, he has served as Deputy Dean and Associate Dean (Education) at the Faculty of Engineering in the University of Sydney. Professor Lim is an Associate Editor for IEEE Potentials, was an Area Editor of the IEEE Transactions on Wireless Communications from September 2013 to September 2018, and previously served as an Associate Editor for the same journal. He has also served as an Associate Editor for IEEE Wireless Communications Letters, Wiley Transactions on Emerging Telecommunications Technologies (ETT), IEEE Signal Processing Letters and IEEE Transactions on Vehicular Technology. He has volunteered on the organizing committee of a number of IEEE conferences, including serving as the TPC co-chair of IEEE Globecom 2017. He chaired the Singapore chapter of the IEEE Communications Society in 2017 and 2018, and is a Distinguished Lecturer of the IEEE Vehicular Technology Society for 2019-20. His research interests span many topics within wireless communications, including cyber-security in the Internet of Things, heterogeneous networks, cooperative transmission, energy-optimized communication networks, multi-carrier modulation, MIMO, cooperative diversity, cognitive radio, and stochastic geometry for wireless networks, and he has published widely in these areas.