Managing Physical Layer Security in Wireless Cellular Networks: A Cyber Insurance Approach

Xiao Lu, Dusit Niyato, *Fellow, IEEE*, Nicolas Privault, Hai Jiang, *Senior Member, IEEE*, and Ping Wang, *Senior Member, IEEE*

***Abstract*—The fifth-generation (5G) wireless networks are expected to provision value-added services with ubiquitous coverage, which makes data security unprecedentedly critical. In this context, physical layer security has emerged as a promising solution to safeguard data transmission by exploiting characteristics of the wireless medium. Despite the recent technological advance in physical layer security and wireless transmission, secrecy outages (i.e., data breaches) and service outages (i.e., connection failures) will inevitably happen and incur financial losses. This economical consequence is a fact that is mostly overlooked by the existing literature. To provide financial protection against secrecy outage and service outage, we introduce a cyber insurance framework for wireless users in cellular networks, where each user pays a premium to an insurer for a future financial compensation if an outage occurs to him/her. In particular, we derive the network risks of the cellular users in terms of secrecy outage probability and service outage probability as well as the financial risk of the cyber insurer in terms of the ruin probability which indicates the chance that the insurer experiences a deficit in affording the losses of outage users. Through numerical evaluation, we demonstrate the impact of network performance on the financial risk of the insurer. The numerical results also show that the ruin probability of the insurer can be effectively reduced by equipping a larger number of antennas at base stations or increasing network frequency reuse.**

Index terms- Physical layer security, cyber insurance, collective risk theory, ruin probability, stochastic geometry.

I. Introduction

Provisioning secured wireless data services with ubiquitous coverage is a pivotal task for the fifth-generation (5G) wireless networks due to the dramatic expansion in wireless access through mobile devices over the Internet. Especially, mobile communication systems are carrying increasingly important confidential information, e.g., for financial transactions, healthcare monitoring, and control, through value-added wireless services such as e-commerce, e-health care, and cloud-based applications. Loss, damage, or delay of such information can cause serious consequences to the users. One evidence is in a recent digital economy survey by Marsh & McLennan [2], which estimated that 445 billion dollars of global financial loss were incurred by cyber risks in 2016. Moreover, in the form of cyber crime, cyber risk damage cost will rise to 6 billion dollars annually by 2021 in which the expenditure on cyber security will become 1 trillion dollars over the years from 2017 to 2021 [3].

Due to the broadcast nature of the wireless medium, a wireless channel is prone to extra cyber risks in wireless physical layer, e.g., caused by eavesdropping and/or jamming, making it challenging to secure data transmission. Traditionally, wireless communication security has been mainly entrusted to encryption implemented in the network layer or application layer, e.g., cryptographic protocols, to secure transmission [4]. However, an encryption process involves a high computational complexity of key distribution and requires a dedicated channel for private key exchanges, which largely hinders its applicabilities for mobile Internet. Alternatively, physical layer security [4]–[6] has emerged and caught significant research attention. It uses channel codes, e.g., Wyner codes [7], to provide direct secure communications. Thus, by exploiting characteristics of the wireless medium (e.g., fading, interference, and noise), physical layer security techniques avoid the use of computation resources (e.g., signal processing on cryptographic keys) and significantly reduce signaling overhead. Therefore, physical layer security can serve as an alternative or complement to the encryption to strengthen wireless security.

Recently, physical layer security in massive multiple-input multiple-output (MIMO) cellular networks has caught increasing attention. As a fundamental enabling technology for 5G communication systems, massive MIMO technology that employs a large-scale antenna array can produce sharp beams in narrow directions, and thus, generate significantly lower information leakage to facilitate physical layer security against eavesdropping [8], [9]. Existing literature has mainly focused on the precoder design for multiuser downlink transmission and artificial-noise (AN)-aided jamming. Secure transmission in a downlink massive MIMO system in the presence of a single eavesdropper with multiple antennas is investigated in [10]–[12]. In [10], a matched-filter precoding scheme is designed, and the system secrecy rate and secrecy outage probability are analyzed. As an extension, the work in [11] first examines different combinations of linear data and artificial noise precoders, and then designs linear precoders based on

Manuscript received September 15, 2017; revised February 1, 2018; accepted February 15, 2018. This work was supported in part by Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, RG 33/16 and MOE2015-T1-2-130 RG122/15, MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, Grant MOE2016-T2-1-036, and NRF2015-NRF-ISF001-2277, and in part by the Natural Sciences and Engineering Research Council of Canada. Some initial results of this paper have been accepted by the IEEE International Conference on Communications in 2018 [1].

X. Lu and H. Jiang are with Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta T6G 1H9, Canada (e-mail: lu9@ualberta.ca; hai1@ualberta.ca).

D. Niyato and P. Wang are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore (e-mail: dniyato@ntu.edu.sg; wangping@ntu.edu.sg).

N. Privault is with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore (e-mail: nprivault@ntu.edu.sg).

matrix polynomials to strike a balance between complexity and performance. In [12], downlink precoder design is investigated in the case with a limited number of RF chains to reduce hardware cost. Lower bounds on the achievable secrecy rate are derived for both analog and hybrid digital/analog precoding. Furthermore, the work in [13] extends the AN-aided jamming design to the scenario with multiple eavesdroppers. Directional jamming is introduced, which injects noise only at selected beams to lower secrecy outage probability in an energy-efficient manner.

Nevertheless, as pointed out in [14], the precoder design of artificial noise usually involves high complexity in large matrix inversion and null-space computation, especially for massive MIMO systems. To address this issue, the work in [14] introduces the use of low transmit power as a way to secure the massive MIMO channels instead of artificial noise injection. It is proven that the power scaling can always guarantee secure transmission if the ratio of the antenna number of the eavesdropper to that of the base station (BS) is below a threshold. Different from aforementioned works on massive MIMO that all consider passive eavesdroppers, the work in [15] investigates the case with an active eavesdropper. The active eavesdropper can perform pilot contamination attacks at the BS by impairing the training signals. Optimal transmit power of the BS allocated for data and artificial noise is derived, as well as the minimum transmit power to guarantee data security. In [16], an overview of detection techniques for active eavesdroppers is presented, and a possible solution to cope with them is discussed.

A. Motivations and Contributions

Although physical layer security techniques manage to improve the robustness and resilience of wireless services, existing cyber risks in cellular networks cannot be completely prevented by developing and deploying system-based security solutions alone. As a result, secrecy outages and service outages (i.e., due to connection failures), which are two typical cyber risks in wireless communication systems, inevitably happen and incur financial losses to the users.

Cyber insurance is a risk management mechanism that transfers the cyber risks undertaken by the insureds to a third-party insurer [17]. It has a potential to eliminate the financial loss of network users incurred from cyber risks. This inspires us to introduce cyber insurance as a solution to protect network users' interest from secrecy outage and service outage as a complement to technological solutions and system approaches (such as physical layer security techniques).

Cyber insurance emerges as one of the most quickly expanding markets of insurance business as indicated by the World Economic Forum [18]. A recent cyber security survey [19] reports that 46% of all UK businesses identified at least one cyber breach or attack in 2016. Moreover, 74% of UK businesses deem cyber security as a high priority for their operation. However, it is challenging to apply cyber insurance to enhance wireless security, due to the difficulty in characterizing and assessing wireless risks [20]. This motivates us to incorporate risk modeling and quantification of cellular networks into a cyber insurance framework.

In this paper, we introduce the concept of cyber insurance to protect wireless users against cyber losses. Our objective is to formulate a cyber insurance framework for risk evaluation and management for future generation wireless systems. In this framework, mobile users can buy cyber insurance from a third-party insurer by paying a certain amount of premium. The insurer then affords the risk of the users and pays indemnities to the users when losses occur to them because of cyber risks. In particular, considering a massive MIMO-enabled cellular network in the presence of eavesdroppers, the insured users' risks are indicated as service unavailability (represented by the service outage probability) and data breach (represented by the secrecy outage probability). Meanwhile, the insurer's risk is measured by the ruin probability [21], i.e., the chance that the insurer is unable to cover all the indemnities. The goal of the cyber insurance framework is to evaluate the risks of both the insured users and insurer. To this end, we focus on investigating the network performance in a large-scale cellular network based on a stochastic geometry analysis. Based on a spatial point process modeling, we characterize the long-term performance of a user in presence of the cyber risks by exploiting statistics of random spatial network distribution and broadcast channels. For cyber insurance, as the losses occur randomly to a population of insured users, we model the stochastic loss claim process of the users based on Cramer-Lundberg model (i.e., compound Poisson model) from collective risk theory [22]. Utilizing the analytical results of network performance, we introduce an analytical approach to evaluate the ruin probability of the insurer.

Important findings from the proposed cyber insurance framework include the following. 1) Larger repulsion in the deployment of BSs contributes to the decrease of the ruin probability while larger repulsion in the deployment of eavesdroppers increases the ruin probability. 2) To manage the ruin probability below a certain level, the indemnities induced by service outages and secrecy outages can be balanced by setting a proper transmission rate of codewords and/or the number of antennas. 3) A high initial reserve is more beneficial to reduce the ruin probability in the case when the indemnity for an outage is relatively high.

In summary, the proposed cyber insurance framework will be useful for both insured users and the insurer. For example, the insured users can be aware of their cyber risk level by evaluating service outage and secrecy outage. The evaluation results would be helpful for the users to make decisions whether or not to purchase cyber insurance. The insurer can assess the capital risks and optimize their portfolio. It is worth noting that this paper is the first work that considers physical layer security from the perspective of both network performance and corresponding financial effects. The proposed unified framework will pave the way to more converged research in wireless security and cyber insurance areas, both of which become more important to sustain reliable and secure next-generation wireless networks.

Notations: In the following, we use $\mathbb{E}[\cdot]$ to denote expectation over all random variables in $[\cdot]$, $\mathbb{E}_X[\cdot]$ to denote the expectation over random variable X, and $\mathbb{P}[Z]$ to denote the probability that an event Z occurs. We denote $\mathcal{G}(\theta, \delta)$

as the gamma distribution with shape parameter θ and scale parameter δ and $\mathcal{E}(a)$ as the exponential distribution with rate parameter a. $\mathbb{1}_{\{\mathbf{A}\}}$ denotes an indicator function that takes the value of 1 if the event $\mathbf{A}$ happens, and takes the value of 0 otherwise. $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{N}$ and $\mathbb{C}$ denote the sets of real numbers, positive real numbers, natural numbers and complex numbers. Besides, $\mathbf{x}_a$ denotes the location of a, and $\|\mathbf{x}_a - \mathbf{x}_b\|$ is used to represent the Euclidean norm between coordinates $\mathbf{x}_a$ and $\mathbf{x}_b$.

II. Related work

Existing literature has investigated insurance for cyber networks, yet almost all of them are for the wired Internet. Cyber insurance differs from traditional insurance in two unique aspects [17]: 1) cyber insurance needs to cover risks caused by smart and intentional attacks instead of natural failures; 2) cyber risks do not have geographical limitations, as simultaneous cyber risks can occur domain-wide, system/platform-wide, or even Internet-wide by virtue of their identical or similar vulnerabilities. Due to these fundamental differences, studies have been conducted to analyze the impact of cyber risks on cyber insurance. In [23], it is revealed that underwriting users with interdependent cyber risks can not only result in improved profit for an insurer but also motivate more efforts by the insured users to improve their security. The reason is that cyber insurance forces the users' joint efforts to reduce correlated risks in exchange for reduced premium payment. In [24], an insurer's preference over risk dependency is studied, by investigating an insurance market consisting of a primary client and a third-party client. The risks of the former are correlated with those of the latter while the latter has independent risks. It is demonstrated that it is more beneficial for the insurer to underwrite both clients, as this reduces the collective risks.

Another mainstream of studies is to explore the benefits of cyber insurance. In [25], an economic model is developed to analyze the benefit of cyber insurance to both insurer and insured users of the Internet. Considering epidemic risks including worms, viruses, and botnet-driven attacks, the model shows that cyber insurance can effectively motivate Internet users to invest in security protection. The work in [26] studies whether or not cyber insurance can improve network security. The analysis indicates that cyber insurance can result in improved network security only when the insurer adopts premium discrimination amongst the insureds. The work in [27] further investigates the effect of moral hazard, which occurs when insureds reduce security protection, which the insurer is unaware of. It is shown that in a market with moral hazard, cyber insurance fails to motivate the insureds to improve security protection. Moreover, the work in [28] provides evidence that cyber insurance can also serve as an incentive for a monopolistic insurer to invest in security, helping the insured users to increase the protection level.

However, to the best of our knowledge, a cyber insurance model for wireless services has not be discussed and introduced before. Moreover, performance modeling to understand the effect of network vulnerability on the insurer's capital risk is missing from the literature. Therefore, they are the focus of this paper.

III. Network Model and Cyber Insurance Framework

In this section, we first introduce the considered system model of a massive MIMO-enabled cellular network in the presence of eavesdroppers. Then, we present the cyber insurance framework as a solution to transfer the cyber risks of the wireless users.

A. Massive MIMO-enabled Cellular Network Model

As shown in Fig. 1, we consider a massive MIMO-enabled cellular network in which all the BSs provision downlink wireless service for users. Each BS is equipped with a large-scale antenna array of L antennas while each user adopts a single antenna. Meanwhile, there exist randomly distributed single-antenna eavesdroppers intending to wiretap the transmitted data from the BSs. The spatial locations of the BSs and eavesdroppers are assumed to follow independent homogeneous α-Ginibre point processes (GPPs) [29], denoted as Φ_B and Φ_E, with spatial densities ρ_B and ρ_E and repulsion factors α_B and α_E, respectively. More details of α-GPP are presented in Section IV-A.

We consider time division duplex (TDD) at the BSs. The channel state information (CSI) estimation can be obtained through uplink training by exploiting the uplink-downlink channel reciprocity [9]. Each BS is considered to have several time-frequency resource blocks. Let N_s denote the maximum number of users that can be supported simultaneously on each resource block. For TDD, N_s is governed by the length of the uplink pilot sequence [30]. The BSs adopt linear zero-forcing beamforming (ZFBF) [31] with equal power per wireless downlink to serve legitimate users simultaneously over a time-frequency resource block[1]. As a result, Gaussian noise or uncorrelated intra-cell interference does not have effects in the massive MIMO regime (i.e., $L \gg N_s \gg 1$) [38]. Besides, all the wireless channels are assumed to follow Rayleigh fading. For cell association, each user is served by a massive MIMO-based BS that provides the strongest average received signal power [39]. For spectrum allocation of each BS, we consider frequency reuse with a factor $\xi \in (0, 1]$. The factor represents the percentage of interfering BSs in the network that are allocated with the same spectrum frequency. We assume the interfering BSs are an independent thinning process of Φ_B. For the analysis of this paper, we focus on a full-load network scenario in which a typical user is served on a resource block with the maximum number of N_s users.

[1]Apart from our adopted ZFBF, other linear precoding schemes, such as maximum ratio transmission (MRT) [32], regularized channel inversion (RCI) [33], and maximum signal-to-leakage-plus-noise ratio (SLNR) [34], and nonlinear precoding schemes, such as Costa precoding [35], can be incorporated into our system model straightforwardly to evaluate the network performance. Furthermore, power allocation of MIMO system can be optimized to reduce service outage probability [36] and secrecy outage probability [37]. We do not evaluate the impact of different precoding schemes or power allocation schemes in this paper as they are out of the scope of this study.

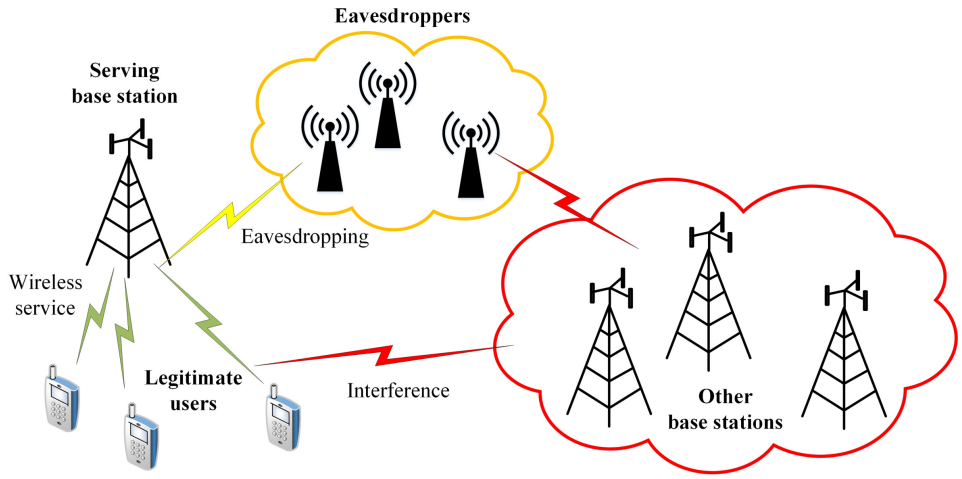


Fig. 1. A cellular network model for downlink service in the presence of eavesdroppers.

TABLE I
NOTATIONS.

Symbol	Definition
Φ_B, Φ_E	The point processes representing the BSs and eavesdroppers, respectively
α_B, α_E	Repulsion factors for the BSs and the eavesdroppers, respectively
P_B	The transmit power of base stations
ρ_B, ρ_E	The density of base stations and eavesdroppers, respectively
L	The number of antennas at a massive MIMO-enabled BS
σ^2	The variance of AWGN
N_s	The number of users simultaneously served by one resource block
η_u, η_e	Received SIR and received SINR of a typical user and an eavesdropper $e \in \Phi_E$, respectively
R_t, R_e	The transmission rate of the codewords and redundant subcodes, respectively

Let P_B denote the transmit power of the BS on each resource block. If a typical user u establishes a downlink connection with the serving BS, denoted as BS 0, its received signal power can be calculated as follows [40, eqn. (1)]:

$$P_{0,u} = \frac{\frac{P_B}{N_s} G\beta}{\|\mathbf{x}_0 - \mathbf{x}_u\|^{\mu}}, \tag{1}$$

where $\frac{P_B}{N_s}$ represents the allocated transmit power to u, $G = L - N_s + 1$ represents the antenna array gain of the massive MIMO-enabled BS adopting ZFBF[2], β is a frequency dependent constant typically calculated as $\frac{3\times10^8}{4\pi\nu}$ [41] with carrier frequency ν, $\mathbf{x}_0$ and $\mathbf{x}_u$ denote the location of the serving BS 0 and user u, respectively, and μ denotes the path-loss exponent.

Let Φ_B^0 denote the set of the BSs that use the same frequency band as that of BS 0. The inter-cell interference observed by a typical user is given by

$$I_u = P_B\beta \sum_{b\in\Phi_B^0} \frac{h_{b,u}}{N_s\|\mathbf{x}_b - \mathbf{x}_u\|^{\mu}}, \tag{2}$$

where $h_{b,u} \sim \mathcal{G}(N_s, 1)$ [36] denotes the channel gain between BS $b \in \Phi_B^0$ and the typical user, and $\mathbf{x}_b$ denotes the location of BS $b \in \Phi_B^0$.

Therefore, the received signal-to-interference-ratio (SIR) at the typical user can be calculated as follows

$$\eta_u = \frac{P_{0,u}}{I_u} = \frac{G\|\mathbf{x}_0 - \mathbf{x}_u\|^{-\mu}}{\sum_{b\in\Phi_B^0} h_{b,u}\|\mathbf{x}_b - \mathbf{x}_u\|^{-\mu}}. \tag{3}$$

The eavesdroppers are considered as non-colluding devices that overhear and intercept the secrecy information of legitimate users individually without active attacks. The received signal-to-interference-plus-noise ratio (SINR) at an eavesdropper $e \in \Phi_E$, is given by

$$\eta_e = \frac{P_B h_{0,e}\beta}{N_s\|\mathbf{x}_0 - \mathbf{x}_e\|^{\mu}(I_e + \sigma^2)}, \tag{4}$$

where $h_{0,e} \sim \mathcal{E}(1)$ [41] is the small-scale fading channel gain between the serving BS 0 of the typical user and an eavesdropper $e \in \Phi_E$, $\mathbf{x}_e$ denotes the location of $e \in \Phi_E$, σ^2 is the variance of additive white Gaussian noise (AWGN), and I_e is the accumulated interference at e expressed as follows:

$$I_e = P_B\beta \sum_{b\in\Phi_B^0} \frac{h_{b,e}}{N_s\|\mathbf{x}_b - \mathbf{x}_e\|^{\mu}}, \tag{5}$$

where $h_{b,e} \sim \mathcal{G}(N_s, 1)$ [41] is the small-scale fading channel gain between the interfering BS $b \in \Phi_B^0$ and eavesdropper

[2]Due to the hardening effect of a massive MIMO channel, the transmitted signals from the BS only undergo long-term effects. Besides, we note that, compared to single-antenna transmission, the average received signal power is scaled by $\frac{(L-N_s+1)}{N_s}$ in massive MIMO transmission with ZFBF.

$e \in \Phi_E$.

We assume that the broadcast channel of each BS is exposed to all the eavesdroppers. In presence of non-colluding eavesdroppers, the secrecy outage probability of a legitimate user is dominated by the most malicious eavesdropper [42], i.e., the eavesdropper that achieves the highest receive SINR, expressed as follows:

$$\eta_{e^\star} = \max_{e \in \Phi_E} \left\{ \frac{P_B h_{0,e} \beta}{N_s \|\mathbf{x}_0 - \mathbf{x}_e\|^\mu (I_e + \sigma^2)} \right\}. \quad (6)$$

Table I summarizes the main notations used in the paper.

B. Cyber Insurance Framework

In this paper, cyber insurance is introduced as a solution to recover the losses from the cyber risks, i.e., secrecy outage and service outage, in the considered system. As shown in Fig. 2, cyber insurance is a mechanism to transfer the risks associated with an insured, e.g., a network user, to a third-party insurer. To establish a cyber insurance contract, an insured pays an upfront premium, in exchange for the insurer's liability of an indemnity payment upon a cyber loss occurrence. For the insured, cyber insurance is to provide financial compensation in the event of a cyber loss at a cost, i.e., premium, to get insurance protection. For the insurer, cyber insurance allows to obtain monetary benefit from the insured in advance, for affording uncertain future risks of the insured.

We consider a cyber insurance framework with cellular network users as the insureds and a third-party corporation other than the service provider as the insurer. Implementing such a cyber insurance framework usually involves a four-step procedure as illustrated in Fig. 3. In Step 1 "Risk Identification", the user identifies its own risk from historical information and network statistics via communication with the service provider, and decides whether to buy a cyber insurance. Once the user determines to buy it, a request is sent to the insurer. In Step 2 "Risk Assessment", upon receiving a request, the insurer needs to assess the potential risks that the user faces by evaluating the conditions of the network. Based on the assessment results, the insurer also needs to evaluate its own exposure to capital risk for carrying the liabilities to the user. In Step 3 "Contract Establishment", after the cyber risks of the user are well investigated, the insurer formulates an insurance contract specifying the liabilities and the amount of indemnity. The contract is validated once the user accepts the conditions of the contract and pays the premium. In Step 4 "Contract Execution", both the insurer and user execute the contract. Once a loss occurs (due to an outage of any type) to the user, a report is made by the user to claim for indemnity payment (Step 4.1 "Claim"). If a service outage is claimed, the insurer confirms with the service provider about the user's loss[3]. If a secrecy outage is claimed, the user needs to provide to the insurer evidence (e.g., the record of illegal transactions) to support the claim (Step 4.2 "Proof of loss"). The indemnity is approved to compensate the user once the loss is affirmed (Step 4.3 "Indemnity").

[3]We assume that the service provider has performance records of its subscribed users. Different techniques [43]–[45] in the existing literature can be employed for service outage detection. However, these techniques are out of the scope of this paper.

IV. Network Service Performance Analysis

In this section, we analyze the performance of users in a large-scale massive MIMO-enabled cellular network. In particular, we consider service outage probability and secrecy outage probability as the performance metrics of the user's risk.

A. Geometric Modeling

In this paper, the performance analysis of the massive MIMO-enabled cellular network is based on α-GPP modeling. α-GPP is a particular type of determinantal point process [46] that abstracts correlation among the randomly located spatial points with a coefficient α ($\alpha = -1/\kappa$ for a positive integer κ). α indicates the repulsion degree of the spatial points which is largest when $\kappa = 1$. The repulsion monotonically decreases with the increase of κ. This converts α-GPP into the widely used Poisson point process (PPP) [47] when κ goes to infinity. Stochastic geometry analysis based on α-GPP provides analytical expressions in terms of Fredholm determinants [48], which is shown to be an efficient way for numerical evaluation of the relevant quantities. Due to its versatility and tractability, α-GPP has recently been widely adopted in modeling cellular networks [49], wireless sensor networks [50], device-to-device communication systems [51], and wireless relay networks [52].

Without loss of generality, we restrict the analysis on a generic point located at $\mathbf{x}$ to an observation window $\mathbb{O}_\mathbf{x}$, denoted as a circular Euclidean plane centered at $\mathbf{x}$ with a positive radius R. For any α-GPP Φ, let ρ denote the spatial density of the points of Φ and $\mathcal{K}$ represent an almost surely finite collection of Φ located inside the observation window $\mathbb{O}_\mathbf{x}$. We introduce here some fundamental properties of α-GPP to facilitate the performance analysis in this paper.

Proposition 1. [53, Lemma 1] *Let r denote the distance between the origin and its closest point in an α-GPP Φ. The probability density function (PDF) of r is given by*

$$f_r(r) = 2\exp(-\pi\rho r^2) \prod_{n\geq 0} \left(1+\alpha\frac{\gamma(n+1,\pi\rho r^2)}{n!}\right)^{-\frac{1}{\alpha}} \times \sum_{n\geq 0} \frac{(\pi\rho)^{n+1} r^{2n+1}}{n!} \left(1+\alpha\frac{\gamma(n+1,\pi\rho r^2)}{n!}\right)^{-1}, \quad (7)$$

where $\gamma(z,a) \triangleq \int_0^a \mathrm{e}^{-t} t^{z-1}\,\mathrm{d}t$, $z \in \mathbb{C}$, $a \geq 0$, denotes the lower incomplete Gamma function.

Proposition 2. [54, Lemma 3] *Let φ represent an arbitrary real-valued function. For an α-GPP Φ, the Laplace transform of $\sum_{k\in\mathcal{K}} \varphi(\mathbf{x}_k)$ can be evaluated as*

$$\mathbb{E}\left[\exp\left(-\sum_{k\in\mathcal{K}} s\varphi(\mathbf{x}_k)\right)\right] = \prod_{n\geq 0}\left(1+\frac{2\alpha(\pi\rho)^{n+1}}{n!} \times \int_0^R \left(1-\exp(-s\varphi(r))\right)\exp(-\pi\rho r^2) r^{2n+1}\mathrm{d}r\right)^{-\frac{1}{\alpha}}. \quad (8)$$

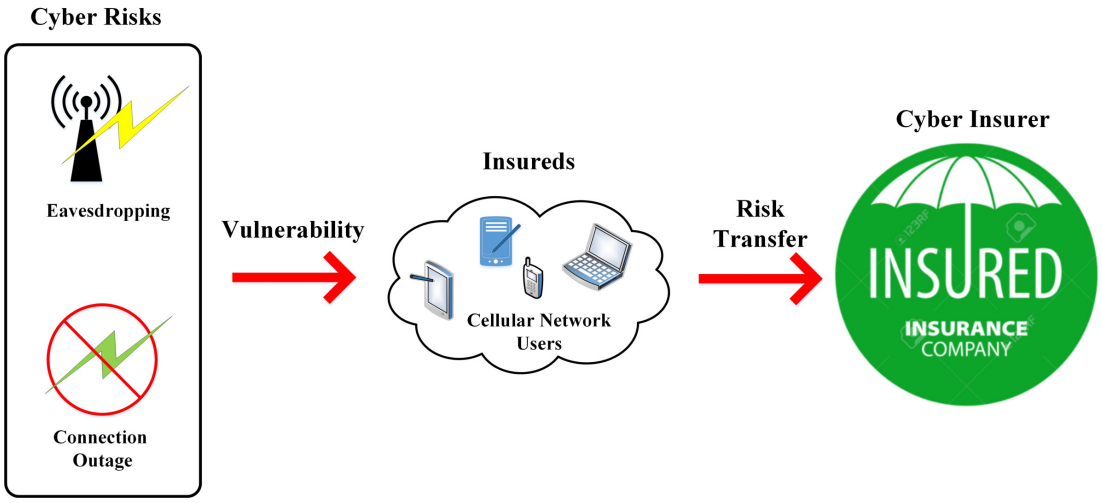


Fig. 2. Illustration of risk transfer of wireless users in the cyber insurance framework.

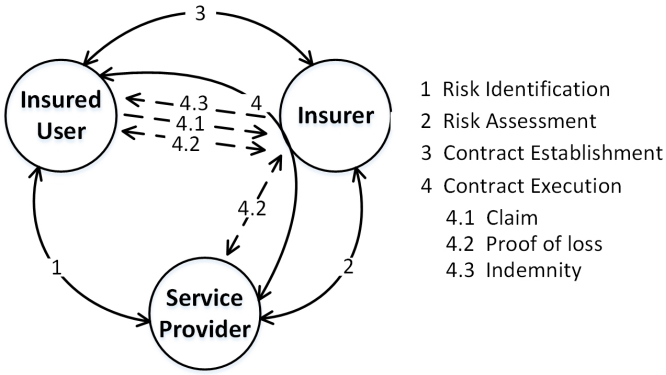


Fig. 3. Procedures of the cyber insurance framework.

B. Performance Metrics

The BSs are considered to adopt the well-known Wyner's encoding scheme [7] to secure confidential information to the legitimate users. In Wyners encoding scheme, a confidential message is associated with a redundant subcode selected randomly from a mother codebook. The subcode introduces randomness to increase eavesdroppers' uncertainty about the transmitted confidential message. Let R_t and R_e denote the transmission rate of the codewords and redundant subcodes, respectively. If the value of R_e is greater than the capacity of the link of the most malicious eavesdropper, information secrecy of a legitimate user can be guaranteed. Otherwise, a secrecy outage occurs.

The wireless service provided by a BS is considered to be unsuccessful if the received SIR at its intended user is lower than a target threshold τ_u. The service outage probability of a typical user is defined as follows:

$$\mathcal{P} \triangleq \mathbb{P}[\eta_u < \tau_u], \tag{9}$$

where η_u is defined in (3), and $\tau_u = 2^{R_t} - 1$.

In the presence of non-colluding eavesdroppers, a secrecy outage occurs to a typical user when the most malicious eavesdropper, denoted as $e^\star$, achieves a received SINR greater than $\tau_e = 2^{R_e} - 1$ [42]. Thus, the secrecy outage probability is defined as follows:

$$\mathcal{O} \triangleq \mathbb{P}[\eta_{e^\star} > \tau_e]. \tag{10}$$

C. Analytical Results

According to the Slivnyaks theorem [55], the analysis of the users' performance is performed for an arbitrary user considered to be located at the origin. We characterize the service outage probability and secrecy outage probability based on α-GPP modeling introduced in Section IV-A as follows.

Theorem 1. *The service outage probability of a typical user in the massive MIMO-enabled cellular network in the presence of malicious eavesdroppers can be expressed as follows:*

$$\mathcal{P} = 1 - 2\int_0^R \exp(-\pi\xi\rho_B r^2) \prod_{n\geq 0}\left(1+\alpha\frac{\gamma(n+1,\pi\xi\rho_B r^2)}{n!}\right)^{-\frac{1}{\alpha}} \times \sum_{n\geq 0}\frac{(\pi\xi\rho_B r)^{n+1} r^n}{n!}\left(1+\alpha\frac{\gamma(n+1,\pi\xi\rho_B r^2)}{n!}\right)^{-1} \times \mathcal{L}^{-1}\left\{\frac{1}{s}\prod_{k\geq 0}\left(1+\frac{2\alpha_B(\pi\xi\rho_B)^{k+1}}{k!}\int_r^R \exp\left(-\pi\xi\rho_B l^2\right) l^{2k+1}\right.\right.$$

$$\times\left[1-\left(1+\frac{s\beta}{N_s l^{\mu}}\right)^{-N_s}\right]\mathrm{d}l\Bigg)^{-\frac{1}{\alpha_B}}\Bigg\}\left(\frac{\beta(L-N_s+1)}{\tau_u N_s r^{\mu}}\right)\mathrm{d}r. \tag{11}$$

where $\mathcal{L}^{-1}\{z\}(x)$ represents the inverse Laplace transform of z evaluated at x.

The proof of **Theorem** 1 is shown in Appendix I.

Theorem 2. *The secrecy outage probability of a typical user in the massive MIMO-enabled cellular network in the presence of malicious eavesdroppers can be expressed as follows:*

$$\mathcal{O}\approx 1-\prod_{k\geq 0}\Bigg[1+\frac{2\alpha_E(\pi\rho_E)^{k+1}}{k!}\int_0^R\prod_{j\geq 0}\Bigg(1+\frac{2\alpha_B(\pi\xi\rho_B)^{j+1}}{j!}$$
$$\times\int_0^R\left(1-\left(1+\frac{\tau_e r^{\mu}}{l^{\mu}}\right)^{-N_s}\right)\exp\left(-\pi\xi\rho_B l^2\right)l^{2j+1}\mathrm{d}l\Bigg)^{-\frac{1}{\alpha_B}}$$
$$\times\exp\left(-\frac{\tau_e N_s r^{\mu}\sigma^2}{P_B\beta}-\pi\rho_E r^2\right)r^{2k+1}\mathrm{d}r\Bigg]^{-\frac{1}{\alpha_E}}. \tag{12}$$

The proof of **Theorem** 2 is provided in Appendix II.

It is noted that, by taking advantage of the stochastic geometry approach, calculation of the service outage probability in (12) does not require the CSI and location information of the eavesdroppers. This is because our proposed cyber insurance framework needs the long-term ergodic performance instead of the instantaneous performance of the cellular network. Moreover, the information of eavesdropper density and repulsion factor are required to evaluate the secrecy outage probability of users. The information can be collected by the BSs. In particular, the presence of an eavesdropper can be detected as its RF front-end may leak the local oscillator power [56]. The BSs can jointly detect the presence of the eavesdroppers to estimate the eavesdroppers' spatial density and repulsion factor, which can be utilized to evaluate the secrecy outage probability of the considered system.

V. Cyber-Insurance and Ruin Probability

We consider a third-party insurer offering a cyber-insurance plan to the cellular users. Each user pays the same premium to the insurer. In the event of a service outage, e.g., because of fading and interference, or a secrecy outage, e.g., because of eavesdropping, the insurer will compensate the user with the corresponding amount of indemnities denoted by $m_{\mathcal{P}}$ and $m_{\mathcal{O}}$, respectively. For the insurer, its income is from U users buying the insurance plan and paying the premium periodically. On the contrary, the expense comes from the indemnities of the users due to outage incidents. The insurer is therefore interested in the ruin which is an event that its capital reserve, i.e., initial reserve plus accumulated income minus aggregate claim amount, becomes negative (i.e., deficit). In the following, we analyze the ruin probability of the insurer [57], [58].

A. Cyber-Insurance Model

Consider that the arrival moments of claims are independent. Denote N_t as the number of claims that arrive from time 0 to time $t\geq 0$. We model $(N_t)_{t\geq 0}$ as a homogeneous Poisson process, and denote its intensity as λ. Let C_k $(k\geq 1)$ denote the k-th claim's amount. C_k's are independent and identically-distributed (i.i.d.). Sequence $(C_k)_{k\geq 1}$ is independent of $(N_t)_{t\in\mathbb{R}_+}$. Also, let

$$Y_k\triangleq\sum_{j=1}^{k}C_j,\qquad k\in\mathbb{N},$$

where $Y_0=0$. Here, Y_k is the aggregate amount of k claims.

The income of the insurer can be represented by a non-decreasing, time-dependent premium function $f:\mathbb{R}_+\to\mathbb{R}_+$. The function maps $t>0$ to the aggregated premium income $f(t)$. The aggregated premium income is received during time 0 and time t given that $f(0)=0$. We assume that the insurer sells an insurance plan with a constant premium rate $c_u>0$ per user per unit time. Thus, we have $f(t)=ct$ with $c\triangleq U\cdot c_u$.

The k-th claim amount, C_k, can take two values $m_{\mathcal{P}}$ and $m_{\mathcal{O}}$ with probabilities p and q, respectively. Here, p and $q=1-p$ denote the conditional probabilities of service outage and secrecy outage, respectively, if an outage occurs. So we have $p=\frac{\mathcal{P}}{\mathcal{P}+\mathcal{O}\cdot p_l}$, where $\mathcal{P}$ is the service outage probability obtained from Theorem 1, and $\mathcal{O}$ is the secrecy outage probability obtained from Theorem 2. Here p_l is the probability that a secrecy outage causes an actual loss to the legitimate user[4], i.e., the eavesdropper exploits the received information for its own benefit and incurs a loss to the user. Then, the intensity of $(N_t)_{t\geq 0}$ can be expressed as $\lambda=\mathcal{P}+\mathcal{O}\cdot p_l$.

Define

$$S(t)=Y_{N_t}=\sum_{k=1}^{N_t}C_k,\qquad t\in\mathbb{R}_+,$$

in which we have $S(t)=0$ if $N_t=0$. According to the compound Poisson risk model, the claim process $(S(t))_{t\in\mathbb{R}_+}$ represents the aggregate claim amount. The claim process is then modeled by the compound Poisson process.

The reserve process $(R_y(t))_{t\geq 0}$ is defined as follows:

$$\begin{aligned}R_y(t)&=y+f(t)-S(t)\\&=y+ct-\sum_{k=1}^{N_t}C_k,\qquad t\geq 0,\end{aligned}\tag{13}$$

where $y\geq 0$ is the amount of initial reserve and $f(t)$ is the aggregated premium obtained during time 0 and time $t>0$.

We consider a finite time horizon denoted by $T>0$. Then, the finite-time ruin probability is expressed as follows [59]:

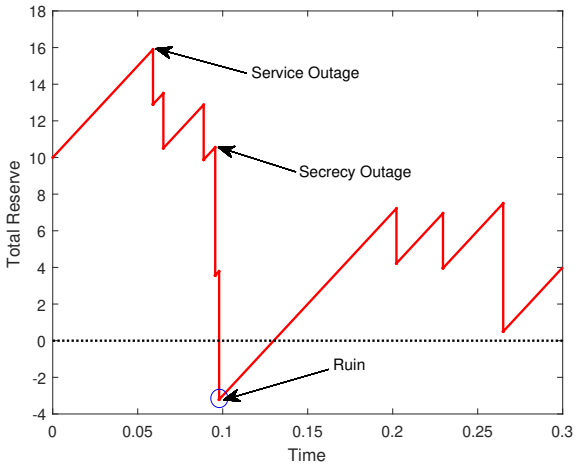
$$\psi(y,T)=\mathbb{P}\big[\ \exists\ t\in[0,T]\ :\ R_y(t)<0\big].$$

Let $y+\mathcal{M}_{[0,T]}$ denote the lowest level of the reserve process in (13) between time 0 and time T, where

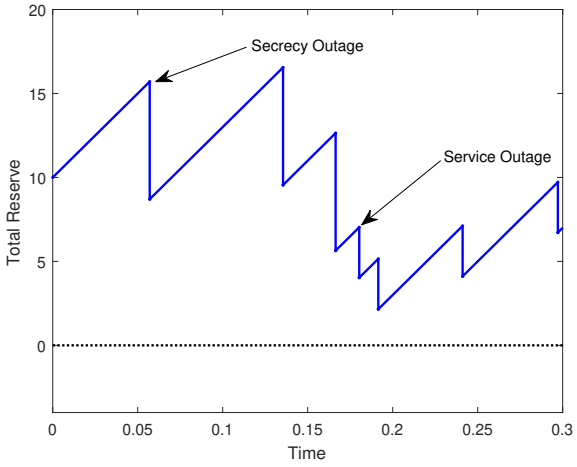
$$\mathcal{M}_{[0,T]}\triangleq\inf\{f(t)-S(t),\quad t\in[0,T]\},\tag{14}$$

which is an explicit probabilistic representation expression that can be used for Monte Carlo simulations.

[4]For a time unit of insurance policy period, p_l can be obtained by dividing the number of claims by the number of secrecy outages. The number of claims can be estimated based on the historical statistics while the number of secrecy outages can be calculated by multiplying the estimated secrecy outage probability in (12) with the total number of insured users.



(a) An example with a ruin event



(b) An example without a ruin event

Fig. 4. Samples of insurers total reserve (Initial reserve $y = 10$, premium rate $c = 1$, $p_l = 1$).

In the compound Poisson risk model, the ruin probability $\psi(y,T)$ is computed as

$$\psi(y,T) = \mathbb{P}\big[\mathcal{M}_{[0,T]} < -y\big], \qquad y \geq 0, \tag{15}$$

and the density of $\mathcal{M}_{[0,T]}$ at $-y < 0$ is expressed as

$$-\frac{\partial \psi(y,T)}{\partial y}. \tag{16}$$

The density of $\mathcal{M}_{[0,T]}$ in (16) indicates the sensitivity of the ruin probability with respect to the initial reserve y. In other words, it shows how fast the ruin probability changes with a certain amount of initial reserve. The density is useful to analyze how the insurer is sensitive to a certain control parameter.

Here, we show an example of the insurer's reserve over time. The indemnities of a service outage and a secrecy outage are set to 3 and 7 monetary units, respectively. With 1000 insured users under service outage probability of 0.01 and secrecy outage probability of 0.01, Figs. 4a and 4b illustrate the insurer's reserves with and without a ruin event, respectively. When an outage of any type, i.e., service outage or secrecy outage, happens to one of the users, the insurer has to pay the corresponding claim, and as such, the reserve sharply drops. A ruin event happens when such a drop makes the reserve fall below zero as shown in the blue circle in Fig. 4a. When a ruin event happens, the insurer does not have enough reserves to pay for the claim. Therefore, it is important to analyze the ruin probability which determines the insurer's vulnerability to insolvency.

B. Calculation of Densities of $\mathcal{M}_{[0,T]}$

In the following, we develop a direct integration by parts method. The method is to numerically compute the non-continuous density functions of the infima of jump processes.

Considering the infimum in (14), we note that $\mathcal{M}_{[0,T]} \leq 0 = f(0)$, and thus $\mathcal{M}_{[0,T]}$ takes non-positive values. On the other hand, we have $\mathcal{M}_{[0,T]} = 0$ if and only if no claim occurs from time 0 to time T (i.e., $N_T = 0$) or the reserve remains non-negative from time 0 and time T, i.e., $f(T_k) - Y_k \geq 0$ for all $k \geq 1$ with $T_k \leq T$. Here T_k denotes the arrival moment of the k-th claim. As a consequence, the probability that $\mathcal{M}_{[0,T]} = 0$ is given by

$$\begin{aligned}
&\mathbb{P}\big[\mathcal{M}_{[0,T]}=0\big] = \mathbb{P}\big[N_T=0\big] + \mathbb{P}\big[\{\mathcal{M}_{[0,T]}\geq 0\}\cap\{N_T\geq 1\}\big] \\
&= e^{-\lambda T} + e^{-\lambda T}\mathbb{E}\Bigg[\sum_{k=1}^{\infty}\lambda^k \int_0^T\int_0^{t_k} \\
&\qquad \cdots \int_0^{t_3}\int_0^{t_2}\prod_{i=1}^{k}\mathbb{1}_{\{f(t_i)>Y_i\}}\mathrm{d}t_1\mathrm{d}t_2\cdots\mathrm{d}t_{k-1}t_k\Bigg] \\
&= e^{-\lambda T} + e^{-\lambda T}\sum_{k=1}^{\infty}\lambda^k \sum_{l_1,\ldots,l_k\in\{0,1\}}\left(\prod_{i=1}^{k} p^{l_i}q^{1-l_i}\right) \\
&\times \int_0^T\int_0^{t_k}\cdots\int_0^{t_3}\int_0^{t_2}\prod_{i=1}^{k}\mathbb{1}_{\{f(t_i)>(m_{\mathcal{P}}-m_{\mathcal{O}})(l_1+\cdots+l_i)+im_{\mathcal{O}}\}} \\
&\qquad \times \mathrm{d}t_1\mathrm{d}t_2\cdots\mathrm{d}t_{k-1}\mathrm{d}t_k. \qquad (17)
\end{aligned}$$

In (17), $t_1, t_2, ..., t_k$ represent the values taken by $T_1, T_2, ..., T_k$, respectively, and l_i $(i = 1, 2, ..., k)$ takes two values: $l_i = 1$ means that the i-th claim is for a service outage, and $l_i = 0$ means that the i-th claim is for a secrecy outage. Thus, the amount of the i-th claim is given by $(m_{\mathcal{P}} - m_{\mathcal{O}})l_i + m_{\mathcal{O}}$.

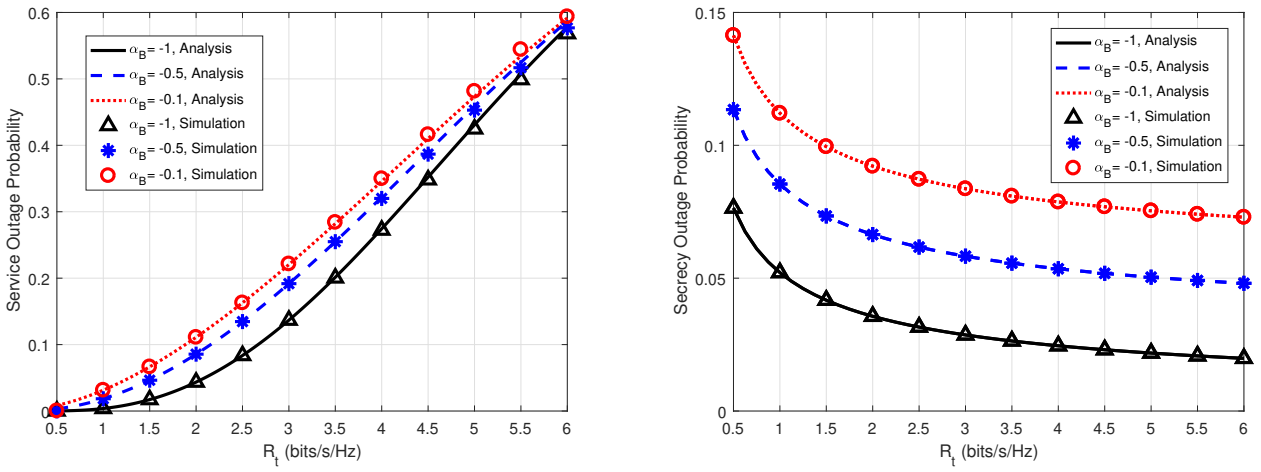
Based on the expression

$$\begin{aligned}
\mathcal{M}_{[0,T]} &= \inf_{0\leq t\leq T}\{f(t) - Y_{N_t}\} = \inf_{T_k\leq T,\ k\geq 0}\{cT_k - Y_k\} \\
&= \mathbb{1}_{\{N_T\geq 1\}}\inf_{T_k\leq T,\ k\geq 1}\{cT_k - \sum_{j=1}^{k} C_k\} \qquad (18)
\end{aligned}$$

of the infimum over the time interval $[0,T]$, we compute the density of $\mathcal{M}_{[0,T]}$, which is efficient for simulations, in the next Proposition.

Proposition 3. *The density of $\mathcal{M}_{[0,T]}$ at $z \in \mathbb{R}$ is given by*

$$\frac{\partial}{\partial z}\mathbb{P}\big[\{\mathcal{M}_{[0,T]}\geq z\}\cap\{N_T\geq 1\}\big]$$



(a) Service outage probability as a function of R_t.

(b) Secrecy outage probability as a function of R_t.

Fig. 5. Impact of α_B ($L = 200$, $N_s = 20$, $\xi = 0.5$, $\rho_E = 10^{-5}$, $R_e = 0.5R_t$).

$$
\begin{aligned}
&= \lambda \mathbb{E}\Bigg[\sum_{j=1}^{N_T} \sum_{l_1,\ldots,l_{1+N_T}\in\{0,1\}} \left(\prod_{i=1}^{1+N_T} p^{l_i} q^{1-l_i} \right) \\
&\qquad \times \mathbb{1}_{\{f(T_{j-1})-(m_{\mathcal{P}}-m_{\mathcal{O}})k_j - j m_{\mathcal{O}} < z \le \varpi_j\}} \Bigg] \\
&\quad + \lambda \mathbb{E}\Bigg[\sum_{l_1,\ldots,l_{1+N_T}\in\{0,1\}} \left(\prod_{i=1}^{1+N_T} p^{l_i} q^{1-l_i} \right) \\
&\qquad \times \mathbb{1}_{\{0<(1+N_T)m_{\mathcal{O}}+(m_{\mathcal{P}}-m_{\mathcal{O}})k_{1+N_T}+z<f(T)\}} \\
&\qquad \times \mathbb{1}_{\{f(T_{N_T})<(1+N_T)m_{\mathcal{O}}+(m_{\mathcal{P}}-m_{\mathcal{O}})k_{N_T+1}+z\}} \\
&\qquad \times \mathbb{1}_{\{z<\inf_{1\le l\le N_T}\{f(T_l)-l m_{\mathcal{O}}-(m_{\mathcal{P}}-m_{\mathcal{O}})k_l\}\}} \Bigg], \qquad (19)
\end{aligned}
$$

where $k_j \triangleq l_1 + \cdots + l_j$, *and*

$$
\begin{aligned}
\varpi_j \triangleq \min\Big\{ &\inf_{1\le l\le j}\{f(T_l) - l m_{\mathcal{O}} - (m_{\mathcal{P}} - m_{\mathcal{O}})k_l\}, \\
&\inf_{j\le l\le N_T}\{f(T_l) - (l+1)m_{\mathcal{O}} - (m_{\mathcal{P}} - m_{\mathcal{O}})k_{l+1}\}\Big\}, \qquad (20)
\end{aligned}
$$

and therein we adopt the convention $\inf_{\emptyset} = +\infty$.

Proposition 3 can be proved as a consequence of Proposition 5 in [57]. We omit the proof of Proposition 3 here to save space.

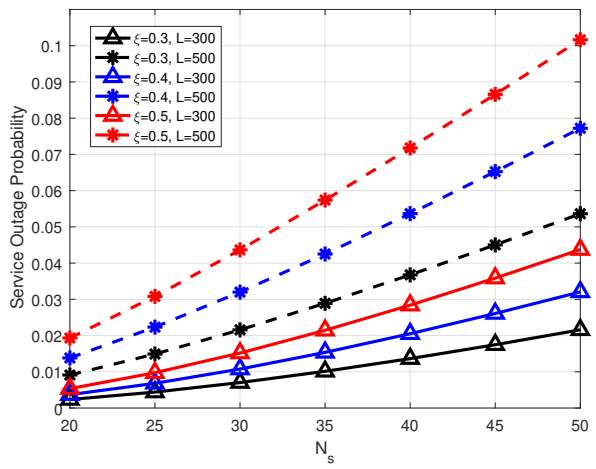
Note that alternative analytical expressions for the density of $\mathcal{M}_{[0,T]}$ are also available in [60], [61].

VI. Numerical Results

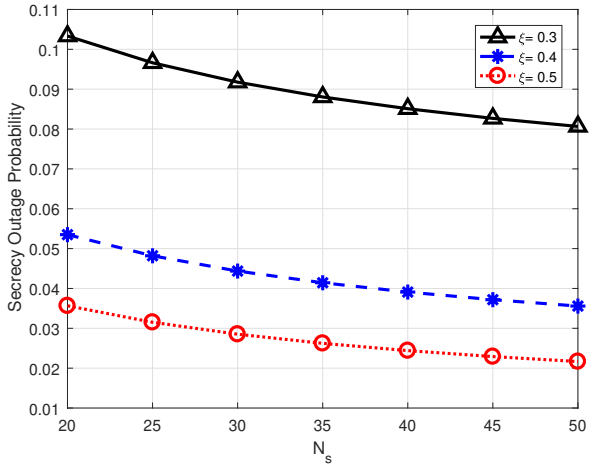
In this section, we numerically evaluate the cyber insurance framework in a massive MIMO-enabled cellular network. We first investigate the impact of network parameters on the service outage probability $\mathcal{P}$ and secrecy outage probability $\mathcal{O}$ obtained in Theorem 1 and Theorem 2, respectively. The density of the BSs is considered as 5×10^{-5} BS/m^2 unless otherwise specified. The bandwidth of and the transmit power on each resource block are 10 MHz and 40 dBm, respectively. The BSs operate on $\nu = 1.8$ GHz frequency. The noise variance is -174 dBm/Hz [62]. The transmission rate of the codewords and redundant subcodes are set at 2 bits/s/Hz and 1 bits/s/Hz, respectively, unless otherwise specified. We first evaluate parameters related to the network deployment, i.e., network repulsion factor α_B and number of antennas L, and resource allocations, i.e., frequency reuse coefficient ξ and the number of users scheduled to serve on each resource block N_s. Fig. 5 validates the accuracy of $\mathcal{P}$ and $\mathcal{O}$ under different α_B. The analytical expressions of $\mathcal{P}$ and $\mathcal{O}$ achieve a close match with the corresponding Monte Carlo simulation results. We observe that deploying BSs more dispersedly, i.e., with large repulsion, helps to decrease both $\mathcal{P}$ and $\mathcal{O}$.

In Fig. 6, we demonstrate $\mathcal{P}$ and $\mathcal{O}$ as functions of N_s. It can be seen that $\mathcal{P}$ increases with N_s and ξ. On the contrary, $\mathcal{O}$ is a decreasing function of N_s and ξ. This can be explained from the fact that scheduling more users on each resource block reduces the transmit power to each user. Moreover, an increment of frequency reuse results in larger aggregated interference to both legitimate users and eavesdroppers. Both factors increase the service outage probability but help to decrease the secrecy outage probability. In addition, the number of antennas L has a non-trivial impact on $\mathcal{P}$, but does not affect $\mathcal{O}$ (as reflected in (12)). The reason is evident that large L increases the antenna array gain for the information signal to the users. Nevertheless, L does not affect the wiretapped signal due to ZFBF.

Then, we examine the impact of deployment factors of eavesdroppers, i.e., spatial density ρ_E and repulsion factor α_E. From (11), the two factors do not affect the service outage probability. We therefore only demonstrate how the secrecy outage probability varies with ρ_E under different values of α_E in Fig. 7. It can be found that larger repulsion in the distribution of the eavesdroppers increases the occurrence of secrecy outage. In other words, the eavesdroppers are the most harmful if they are scattered evenly with the largest repulsion factor $\alpha_E = -1$. Moreover, the eavesdroppers are



(a) Service outage probability as a function of N_s.



(b) Secrecy outage probability as a function of N_s ($L = 200$).

Fig. 6. Impacts of N_s, ξ and L ($\rho_E = 10^{-5}$).

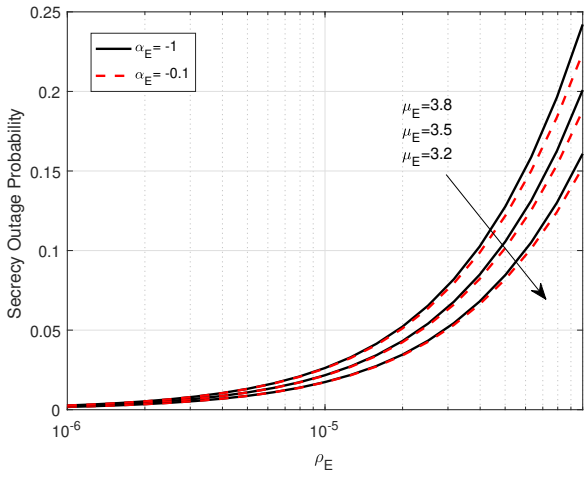


Fig. 7. Secrecy outage probability as a function of ρ_E ($\rho_B = 1 \times 10^{-4}$, $L = 200$, $N_s = 50$, $\xi = 0.5$).

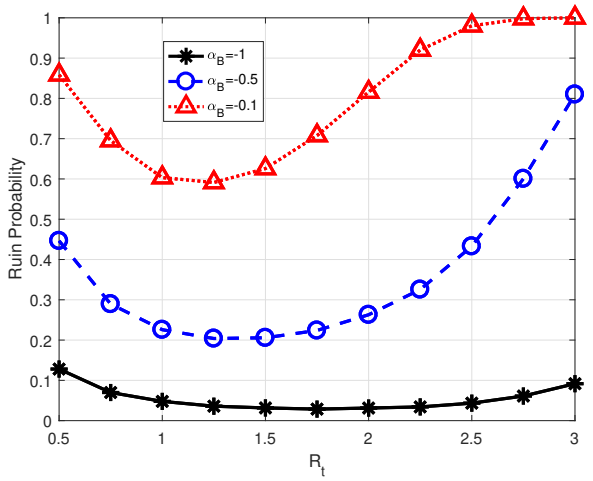


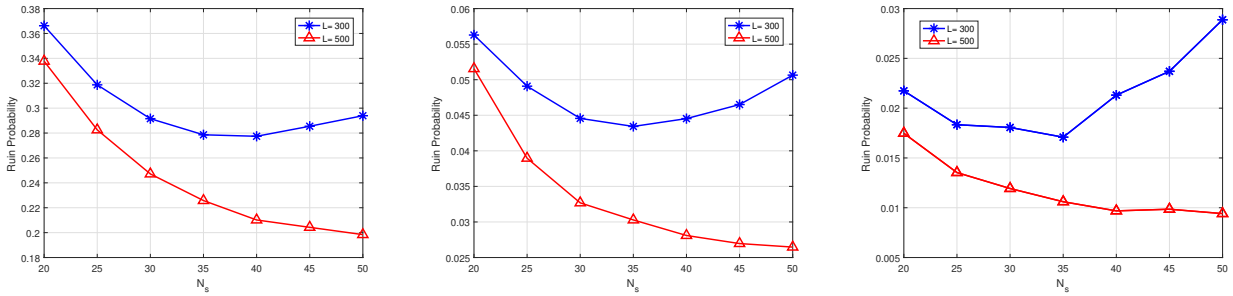
Fig. 8. Ruin probability as a function of R_t ($p_l = 1$).

more malicious if they are deployed in the locations with a larger path-loss exponent. This is because in a massive MIMO-enabled cellular network with ZFBF transmission, interference dominates the wiretapped signals. A larger path exponent helps to attenuate the aggregated interference which benefits eavesdropping.

Based on the network performance evaluation, we study the risk of the insurer by evaluating its ruin probability ψ in (15). The indemnities of a service outage and a secrecy outage are set to 3 and 7 monetary unit unless otherwise specified. We first focus on the influence of network parameters. Fig. 8 depicts how the ruin probability varies with R_t under different α_B. We note that there might exist a minimum of ψ with respect to R_t. This can be understood from Fig. 5 that $\mathcal{P}$ is an increasing function while $\mathcal{O}$ is a decreasing function of R_t. As a result, when R_t is small and large, we have high $\mathcal{O}$ and high $\mathcal{P}$, respectively, both leading to high ruin probability. This indicates that the ruin probability can be minimized by setting a proper code rate R_t.

Fig. 9 compares the ruin probability under different frequency reuse coefficient ξ. Similar to Fig. 8, there might also exist a minimum of the ruin probability with respect to N_s. This is due to the fact that the increase of N_s results in larger $\mathcal{P}$ but lower $\mathcal{O}$ as shown in Fig. 6. Moreover, employing a larger number of antennas contributes to smaller ruin probability as the service outage probability can be mitigated. Interestingly, the ruin probability decreases with the increase of ξ. This is due to the fact that the indemnity of secrecy outage probability $\mathcal{O}$ is much larger than that of service outage probability $\mathcal{P}$. Therefore, though a larger ξ increases $\mathcal{P}$ and decreases $\mathcal{O}$, the effect of $\mathcal{O}$ dominates that of $\mathcal{P}$ on the ruin probability. This indicates that, in practice, heavy frequency reuse in the emerging ultra-dense cellular networks benefits the cyber insurer.

Fig. 10 shows the impact of the density of eavesdroppers ρ_E on the ruin probability ψ. It can be found that ψ increases



(a) $\xi = 0.3$ (b) $\xi = 0.4$ (c) $\xi = 0.5$

Fig. 9. Ruin probability as a function of N_s ($p_l = 1$).

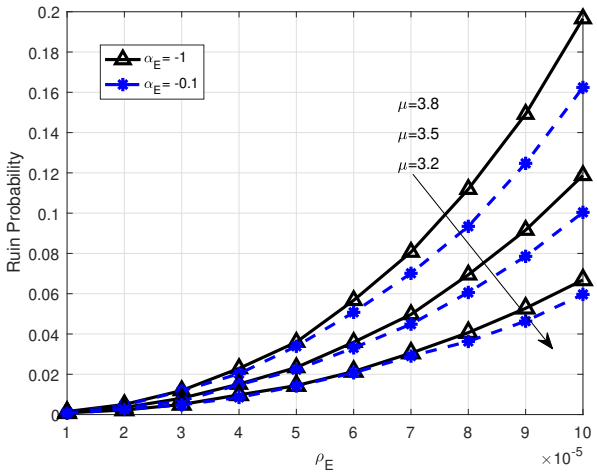


Fig. 10. Ruin probability as a function of the density of eavesdroppers ($p_l = 0.3$).

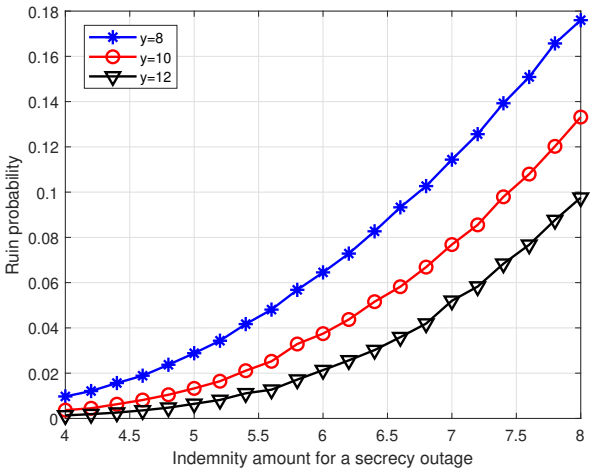


Fig. 11. Ruin probability as a function of the indemnity amount for a secrecy outage ($m_{\mathcal{P}} = 3$, $p_l = 1$).

exponentially with ρ_E. This implies that increasing the density of eavesdroppers is more disruptive to the insurer when ρ_E becomes larger.

Next, we demonstrate the effects of indemnity and initial reserve on the ruin probability in Fig. 11. The indemnity of a service outage $m_{\mathcal{P}}$ is fixed at 3 while that of secrecy outage $m_{\mathcal{O}}$ varies from 4 to 8. It is found that the impact of $m_{\mathcal{P}}$ on the ruin probability becomes more pronounced with the increase of $m_{\mathcal{P}}$. Additionally, it is evident that increasing the initial reserve is an effective way to lower the ruin probability especially when the indemnity is large. However, such a large initial reserve incurs a substantial opportunity cost to the insurer as the reserve cannot be used for financial investment to generate another stream of revenue.

Fig. 12 shows the density of $\mathcal{M}_{[0,T]}$ as a function of premium rate c_u with different initial reserve y. It is observed that the density of $\mathcal{M}_{[0,T]}$ is a decreasing function of the premium rate. When the premium rate is small, the density of $\mathcal{M}_{[0,T]}$ is very sensitive to the amount of initial reserve. This indicates that when the premium income of the insurer is low, a small decrease of the initial reserve can result in a significant increase in the ruin probability. This sensitivity analysis is helpful for the insurer to set a proper premium rate based on its initial reserve to control the variation of ruin probability. For example, considering an uncertainty that the available initial reserve could vary from 8 to 12, in order to control the sensitivity of ruin probability within 0.01, the insurer should charge a premium rate no less than 0.425.

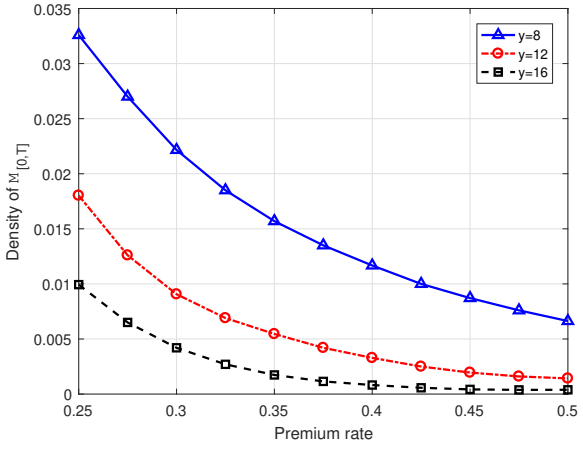


Fig. 12. Density of $\mathcal{M}_{[0,T]}$ as a function of premium rate c_u.

VII. Conclusion

In this paper, we present a cyber insurance framework for wireless services, in which the network users pay a premium to the insurer in order to protect themselves from the loss due to cyber risks. Specifically, considering secrecy outage and service outage as the cyber risks, we introduce a quantitative approach to assess the vulnerabilities of insured users in the subscribed network and in turn the capital risks carried by the third-party insurer. The combination of network analysis and economic analysis provides insights to understand the interplay between wireless systems and cyber insurance business. Our proposed cyber insurance framework is general and can be customized to different emerging network scenarios for future generation networks. The analysis can be useful for further optimization of the benefits of the insurer and/or insureds, which will be one of our future research directions.

Appendix I: Proof of **Theorem 1**

Proof. Let $r_{0,u} = \|\mathbf{x}_0 - \mathbf{x}_u\|$. Following the definition of service outage probability in (9), we have

$$\begin{aligned}\mathcal{P} &= \mathbb{P}\left[\frac{P_B\beta(L-N_s+1)r_{0,u}^{-\mu}}{N_s I_u} < \tau_u\right] \\ &= \mathbb{E}_{r_{0,u}}\left[\mathbb{P}\left[\frac{I_u}{P_B} > \frac{\beta(L-N_s+1)}{\tau_u N_s r_{0,u}^{\mu}}\middle| r_{0,u}\right]\right] \\ &= 1 - \int_0^{\infty} F_{\frac{I_u}{P_B}|r_{0,u}}\left(\frac{\beta(L-N_s+1)}{\tau_u N_s r^{\mu}}\right) f_{r_{0,u}}(r)\mathrm{d}r, \quad (21)\end{aligned}$$

where $F_{\frac{I_u}{P_B}|r_{0,u}}(x)$ is the conditional cumulative distribution function (CDF) of $\frac{I_u}{P_B}$ given $r_{0,u}$, and $f_{r_{0,u}}(r)$ is the PDF of $r_{0,u}$ which can be expressed as follows from Proposition 1.

$$\begin{aligned}f_{r_{0,u}}(r) &= 2\exp(-\pi\rho_B r^2)\prod_{n\geq 0}\left(1+\alpha\frac{\gamma(n+1,\pi\rho_B r^2)}{n!}\right)^{-\frac{1}{\alpha}} \\ &\times \sum_{n\geq 0}\frac{(\pi\rho_B r)^{n+1}r^n}{n!}\left(1+\alpha\frac{\gamma(n+1,\pi\rho_B r^2)}{n!}\right)^{-1}. \quad (22)\end{aligned}$$

Let $\mathcal{L}_{I_u}(s) = \mathbb{E}[\exp(-sI_u)]$ denote the Laplace transform of I_u evaluated at s. By the definition of Laplace transform, the conditional CDF of $\frac{I_u}{P_B}$ can be calculated as follows:

$$\begin{aligned}F_{\frac{I_u}{P_B}|r_{0,u}}(x) &= \mathcal{L}^{-1}\left\{\frac{1}{s}\mathcal{L}_{\frac{I_u}{P_B}}(s)\right\}(x) \\ &= \mathcal{L}^{-1}\left\{\frac{1}{s}\mathbb{E}\left[\exp\left(-\frac{sI_u}{P_B}\right)\right]\right\}(x) \\ &= \mathcal{L}^{-1}\left\{\frac{1}{s}\mathbb{E}\left[\exp\left(-s\beta\sum_{b\in\Phi_B^0}\frac{h_{b,u}}{N_s\|\mathbf{x}_b-\mathbf{x}_u\|^{\mu}}\right)\right]\right\}(x) \\ &= \mathcal{L}^{-1}\left\{\frac{1}{s}\mathbb{E}\left[\prod_{b\in\Phi_B^0}M_{h_{b,u}}\left(-\frac{s\beta}{N_s\|\mathbf{x}_b-\mathbf{x}_u\|^{\mu}}\right)\right]\right\}(x), \quad (23)\end{aligned}$$

where $M_{h_{b,u}}(\cdot)$ is the MGF of $h_{b,u}$. Since $h_{b,u}\sim\mathcal{G}(N_s,1)$, $M_{h_{b,u}}(\cdot)$ can be calculated as $M_{h_{b,u}}(z) = (1-z)^{-N_s}$. Therefore, we have

$$\begin{aligned}F_{\frac{I_u}{P_B}|r_{0,u}}(x) &= \mathcal{L}^{-1}\left\{\frac{1}{s}\mathbb{E}\left[\prod_{b\in\Phi_B^0}\left(1+\mathbb{1}_{\{\|\mathbf{x}_b-\mathbf{x}_u\|>r_{0,u}\}}\right.\right.\right. \\ &\left.\left.\left.\times\frac{s\beta}{N_s\|\mathbf{x}_b-\mathbf{x}_u\|^{\mu}}\right)^{-N_s}\right]\right\}(x) \\ &\overset{(a)}{=}\mathcal{L}^{-1}\left\{\frac{1}{s}\prod_{k\geq 0}\left(1+\frac{2\alpha_B(\pi\xi\rho_B)^{k+1}}{k!}\right.\right. \\ &\times\int_0^R\left[1-\left(1+\frac{\mathbb{1}_{\{l>r_{0,u}\}}s\beta}{N_s l^{\mu}}\right)^{-N_s}\right]\exp\left(-\pi\xi\rho_B l^2\right) \\ &\left.\left.\times l^{2k+1}\mathrm{d}l\right)^{-\frac{1}{\alpha_B}}\right\}(x) \\ &=\mathcal{L}^{-1}\left\{\frac{1}{s}\prod_{k\geq 0}\left(1+\frac{2\alpha_B(\pi\xi\rho_B)^{k+1}}{k!}\int_{r_{0,u}}^R\left[1-\left(1+\frac{s\beta}{N_s l^{\mu}}\right)^{-N_s}\right]\right.\right. \\ &\left.\left.\times\exp\left(-\pi\xi\rho_B l^2\right)l^{2k+1}\mathrm{d}l\right)^{-\frac{1}{\alpha_B}}\right\}(x), \quad (24)\end{aligned}$$

where (a) follows Proposition 2.

Plugging (24) and (22) into (21), we have the result in (11), which concludes the proof. □

Appendix II: Proof of **Theorem 2**

Proof. Since all the eavesdroppers can wiretap the broadcast information from BS 0 and receive interference from the same set of interfering BSs, there exists a correlation among the SINR at the eavesdroppers. However, this correlation is strongly weakened by the channel fading and the eavesdroppers' random spatial locations. In the following, we use an approximation that the interference received at the eavesdroppers are independent for analytical tractability. We validate that this approximation is tight through numerical results in Section VI.

According to the definition in (10), we can derive the secrecy outage probability as follows:

$$\begin{aligned}\mathcal{O} &= \mathbb{P}[\eta_{e^\star} > \tau_e] = 1 - \mathbb{P}[\eta_{e^\star} \leq \tau_e] \\ &= 1 - \mathbb{P}\left[\max_{e\in\Phi_E}\left\{\frac{P_B h_{0,e}\beta}{N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}(I_e+\sigma^2)}\right\}\leq\tau_e\right] \\ &= 1 - \mathbb{E}\left[\prod_{e\in\Phi_E}\mathbb{P}\left[h_{0,e}\leq\frac{\tau_e N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}(I_e+\sigma^2)}{P_B\beta}\right]\right] \\ &\overset{(b)}{=} 1 - \mathbb{E}\left[\prod_{e\in\Phi_E}\mathbb{E}_{I_e}\left[1-\exp\left(-\frac{\tau_e N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}I_e}{P_B\beta}\right)\right.\right. \\ &\left.\left.\times\exp\left(-\frac{\tau_e N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}\sigma^2}{P_B\beta}\right)\right]\right] \\ &= 1 - \mathbb{E}\left[\prod_{e\in\Phi_E}\left(1-\mathcal{L}_{I_e}\left(\frac{\tau_e N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}}{P_B\beta}\right)\right.\right. \\ &\left.\left.\times\exp\left(-\frac{\tau_e N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}\sigma^2}{P_B\beta}\right)\right)\right] \\ &= 1 - \mathbb{E}\left[\exp\left(\sum_{e\in\Phi_E}\ln\left(1-\mathcal{L}_{I_e}\left(\frac{\tau_e N_s\|\mathbf{x}_0-\mathbf{x}_e\|^{\mu}}{P_B\beta}\right)\right.\right.\right.\end{aligned}$$

$$\times \exp\left(-\frac{\tau_e N_s \|\mathbf{x}_0-\mathbf{x}_e\|^\mu \sigma^2}{P_B\beta}\right)\Big)\Big)\Big]$$

$$\overset{(c)}{\approx} 1-\prod_{k\geq 0}\Bigg(1+\frac{2\alpha_E(\pi\rho_E)^{k+1}}{k!}\int_0^R \mathcal{L}_{I_e}\left(\frac{\tau_e N_s r^\mu}{P_B\beta}\right) \times \exp\left(-\frac{\tau_e N_s r^\mu \sigma^2}{P_B\beta}-\pi\rho_E r^2\right) r^{2k+1}\mathrm{d}r\Bigg)^{-\frac{1}{\alpha_E}}, \quad (25)$$

where $\mathcal{L}_{I_e}\left(\frac{\tau_e N_s r^\mu}{P_B\beta}\right)$ is the Laplace transform of I_e evaluated at $\frac{\tau_e N_s r^\mu}{P_B\beta}$, (b) follows the CDF of $h_{0,e} \sim \mathcal{E}(1)$, i.e., $\mathbb{P}[h_{0,e} \leq x] = 1-\exp(-x)$, and (c) follows the approximation that the interference received at each eavesdropper is independent and applies Proposition 2.

We then continue to characterize the Laplace transform of I_e as follows:

$$\begin{aligned}
\mathcal{L}_{I_e}(s) &= \mathbb{E}\left[\exp\left(-sI_e\right)\right] \\
&= \mathbb{E}\left[\prod_{b\in\Phi_B^0}\exp\left(-\frac{sP_B h_{b,e}\beta}{N_s\|\mathbf{x}_b-\mathbf{x}_e\|^\mu}\right)\right] \\
&= \mathbb{E}\left[\prod_{b\in\Phi_B^0} M_{h_{b,e}}\left(-\frac{sP_B\beta}{N_s\|\mathbf{x}_b-\mathbf{x}_e\|^\mu}\right)\right] \\
&= \mathbb{E}\left[\prod_{b\in\Phi_B^0}\left(1+\frac{sP_B\beta}{N_s\|\mathbf{x}_b-\mathbf{x}_e\|^\mu}\right)^{-N_s}\right] \\
&= \prod_{j\geq 0}\Bigg(1+\frac{2\alpha_B(\pi\xi\rho_B)^{j+1}}{j!}\int_0^R\left[1-\left(1+\frac{sP_B\beta}{N_s l^\mu}\right)^{-N_s}\right] \\
&\qquad \times \exp\left(-\pi\xi\rho_B l^2\right) l^{2j+1}\mathrm{d}l\Bigg)^{-\frac{1}{\alpha_B}}, \quad (26)
\end{aligned}$$

in which the last equality applies Proposition 2.

Finally, inserting (26) into (25) yields the result in (12). □

REFERENCES

[1] X. Lu, D. Niyato, N. Privault, H. Jiang, and S. S. Wang, "A cyber insurance approach to manage physical layer secrecy for massive MIMO cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, May 2018.

[2] Marsh & McLennan, *MMC Cyber Handbook 2016*. Accessed on September 14th, 2017. [Online] Available: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf.

[3] S. Morgan, Top 5 cybersecurity facts, figures and statistics for 2017. [Online]. Available: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html.

[4] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 1027-1053, Second Quarter 2017.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014.

[6] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, Apr. 2011.

[7] A. D. Wyner,"The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[8] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?," *IEEE J. Sel. Areas Commun.* vol. 32, no. 6, pp. 1065-1082, June 2014.

[9] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of BS antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590-3600, Nov. 2010.

[10] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multi-cell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766-4781, Sept. 2014.

[11] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245-2261, Mar. 2016.

[12] J. Zhu, W. Xu, and N. Wang, "Secure massive MIMO systems with limited RF chains," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5455-5460, June 2017.

[13] J. Wang, J. Lee, F. Wang, T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854-6868, Dec. 2015.

[14] J. Zhu, and W. Xu, "Securing massive MIMO via power scaling," *IEEE Commun. Letters*, vol. 20, no. 5, pp. 1014-1017, May 2016.

[15] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880-3900, July 2016.

[16] D. Kapetanovic, G. Zheng, F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21-27, June 2015.

[17] X. Lu, D. Niyato, H. Jiang, P. Wang, and H. V. Poor, "Cyber insurance for heterogeneous wireless networks," *IEEE Commun. Mag.*, accepted.

[18] Global risks 2017. Technical report. World Economic Forum, Geneva. [Online] Available: http://www3.weforum.org/docs/GRR17_Report_web.pdf.

[19] 2017 Information Security Breaches Survey. Technical report, UK HM Government. [Online] Available: https://www.ipsos.com/sites/default/files/2017-04/sri-cybersecurity-breaches-survey-2017.pdf.

[20] I. A. Tondel, F. Seehusen, E. A. Gjare, and M. E. G. Moe, "Differentiating cyber risk of insurance customers: The insurance company perspective," In *Proc. Int. Conf. Availability, Reliability, and Security*, Reggio Calabria, Italy, Aug. 2016.

[21] D. C. M. Dickson, *Insurance Risk and Ruin*, Cambridge University Press, Nov. 2010.

[22] T. Mikosch, *Non-life insurance mathematics: An introduction with the Poisson process*. Springer Science & Business Media, 2009.

[23] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies in the presence of security interdependence," in *Proc. 12th Workshop on the Economics of Networks, Systems and Computation*, New York, USA, June 2017.

[24] M. M. Khalili, P. Naghizadeh, and M. Liu, "Embracing risk dependency in designing cyber-insurance contracts," in *Proc.55th Annual Allerton Conf. Commun., Control, and Computing (Allerton)*, Monticello, IL, USA, Oct. 2017.

[25] M. Lelarge and J. Bolot, "Economic incentives to increase security in the Internet: The case for insurance," in *Proc. IEEE Conf. Computer Commun. (INFOCOM)*, Rio de Janeiro, Brazil, Apr. 2009.

[26] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? A market analysis," in *Proc. IEEE Conf. Computer Commun. (INFOCOM)*, Toronto, ON, May 2014.

[27] Z. Yang, and J. C. S. Lui, "Security adoption and influence of cyber-insurance markets in heterogeneous networks," *Performance Evaluation*, vol. 74, pp. 1-17, Apr. 2014.

[28] A. Laszka and J. Grossklags, "Should cyber-insurance providers invest in software security," in *European Symposium on Research in Computer Security*, Springer International Publishing, 2015.

[29] L. Decreusefond, I. Flint, N. Privault, and G. L. Torrisi, "Determinantal point processes," *Advances in applied probability*, vol. 52, no. 4, Aug. 2015.

[30] Q. Ye, O. Y. Bursalioglu, H. C. Papadopoulos, C. Caramanis, and J. G. Andrews, "User association and interference management in massive MIMO HetNets," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2049-2065, May 2016.

[31] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Processing*, vol. 52, no. 2, pp. 461-471, Jan. 2004.

[32] J. Park, N. Lee, J. G. Andrews, and R. W. Heath, "On the optimal feedback rate in interference-limited multi-antenna cellular systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5748-5762, Aug. 2016.

[33] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006-2021, June 2014.

[34] A. M. Alam, P. Mary, J. Y. Baudais, and X. Lagrange, "Asymptotic analysis of area spectral efficiency and energy efficiency in PPP networks with SLNR precoder," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3172-3185, July 2017.

[35] S. T. Veetil, K. Kuchi, and R. K. Ganti, "Coverage analysis of cloud radio networks with finite clustering," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 594-606, Jan. 2017.

[36] S. Akbar, Y. Deng, A. Nallanathan, M. Elkashlan, and G. K. Karagiannidis, "Massive multiuser MIMO in heterogeneous cellular networks with full duplex small cells," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4704-4719, Nov. 2017.

[37] K. Guo, Y. Guo, and G. Ascheid, "Security-constrained power allocation in MU-massive-MIMO with distributed antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8139-8153, Dec. 2016.

[38] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436-1449, Apr. 2013.

[39] D. Bethanabhotla, O. Y. Bursalioglu, H. C. Papadopoulos, and Giuseppe Caire, "Optimal user-cell association for massive MIMO wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1835-1850, Mar. 2016.

[40] A. He, L. Wang, M. Elkashlan, Y. Chen, K.-K. Wong, "Spectrum and energy efficiency in massive MIMO enabled HetNets: A stochastic geometry approach," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2294-2297, Dec. 2015.

[41] L. Wang, K. K. Wong, M. Elkashlan, A. Nallanathan, and S. Lambotharan, "Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1375-1389, Aug. 2016.

[42] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[43] W. Wang, Q. Lia, and Q. Zhang "COD: A cooperative cell outage detection architecture for self-organizing femtocell networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6007-6014, Nov. 2014.

[44] I. de-la-Bandera, R. Barco, P. Muoz, and I. Serrano, "Cell outage detection based on handover statistics," *IEEE Commun. Letters*, vol. 19, no. 7, pp. 1189-1192, July 2015.

[45] A. Zoha, A. Saeed, A. Imran, M. A. Imran, and A. A. Dayya, "Data-driven analytics for automated cell outage detection in self-organizing networks," in *Proc. Int. Conf. Design of Reliable Communication Networks*, Kansas City, MO, USA, Mar. 2015.

[46] L. Decreusefond, I. Flint, and A. Vergne, "Efficient simulation of the Ginibre point process." *Adv. Appl. Probab.*, vol. 52, no. 4, pp. 1003-1012, Oct. 2015.

[47] H. ElSawy, A. Sultan-Salem, M.-S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 1, pp. 167-203, First Quarter 2017.

[48] T. Shirai and Y. Takahashi, "Random point fields associated with certain fredholm determinants I: Fermion, Poisson and Boson point processes," *Journal of Functional Analysis*, vol. 205, no. 2, pp. 414-463, Dec. 2003.

[49] X. Lu, I. Flint, D. Niyato, N. Privault and P. Wang, "Self-sustainable communications with RF energy harvesting: Ginibre point process modeling and analysis," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1518-1535, May 2016.

[50] I. Flint, X. Lu, N. Privault, D. Niyato, and P. Wang, "Performance analysis of ambient RF energy harvesting with repulsive point process modelling," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5402-5416, May 2015.

[51] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and Z. Han, "Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis," *IEEE Trans. Wireless Commun.*, accepted.

[52] X. Lu, G. Li, H. Jiang, D. Niyato, and P. Wang, "Analysis of wireless-powered relaying with ambient backscattering," in *Proc. IEEE ICC*, Kansas city, MO, May 2018.

[53] H. B. Kong, P. Wang, D. Niyato, and Y. Cheng, "Modeling and analysis of wireless sensor networks with/without energy harvesting using Ginibre point processes," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3700-3713, June 2017.

[54] H. B. Kong, I. Flint, P. Wang, D. Niyato, and N. Privault, "Exact performance analysis of ambient RF energy harvesting wireless sensor networks with Ginibre point process," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3769-3784, Oct. 2016.

[55] M. Haenggi, *Stochastic Geometry for Wireless Networks*, Cambridge University Press New York, NY, USA.

[56] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Japan, Mar. 2012.

[57] S. Loisel and N. Privault, "Sensitivity analysis and density estimation for finite-time ruin probabilities," *Journal of Computational and Applied Mathematics archive*, vol. 230, no. 1, pp. 107-120, Aug. 2009.

[58] D. C. M. Dickson, *Insurance Risk and Ruin*, Cambridge University Press, Nov. 2010.

[59] P. Picard and C. Lefèvre, "The probability of ruin in finite time with discrete claim size distribution," *Scandinavian Actuarial Journal*, vol. 1, no. 1, pp. 58-69, 1997.

[60] M. Dozzi and P. Vallois, "Level crossing times for certain processes without positive jumps," *Bulletin des sciences mathématiques*, vol. 121, no. 5, pp. 355-376, 1997.

[61] J. A. León and J. Villa, "On the distributions of the sup and inf of the classical risk process with exponential claim," *Communications on Stochastic Analysis*, vol. 3, no. 1, pp. 69-84, 2009.

[62] K. Hosseini, W. Yu, and R. S. Adve, "Large-scale MIMO versus network MIMO for multicell interference mitigation," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 5, pp. 930-941, Oct. 2014.