A Cyber Insurance Approach to Manage Physical Layer Secrecy for Massive MIMO Cellular Networks

Xiao Lu[†], Dusit Niyato[‡], Nicolas Privault[⋆], Hai Jiang[†], and Shaun S. Wang[≀]
[†] Dept. of Electrical & Computer Engineering, University of Alberta, Canada
[‡] School of Computer Science and Engineering, Nanyang Technological University, Singapore
[⋆] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[≀] Division of Banking & Finance, Nanyang Business School (NBS), Singapore

Abstract—**Due to the fading and broadcast nature of wireless medium, it is challenging to provide full wireless coverage and secure the transmitted signals from unintended users in cellular networks. As a result, cyber risks, such as service outage and secrecy outage, would inevitably occur and cause loss/damage to the users. To transfer the cyber risks and mitigate the impact of loss, cyber insurance appears to be a promising solution for the economics of wireless services. In this paper, we introduce a cyber insurance framework for wireless users to relieve loss from the cyber risks. In this framework, each user pays a premium to an insurer. If the user experiences an outage, he/she will claim the loss, and the insurer will pay the corresponding indemnity to the user. Under the network model of a large-scale massive multiple-input multiple-output (MIMO) cellular networks and cyber insurance, we first characterize the user performance in terms of both service outage probability and secrecy outage probability using stochastic geometry analysis. Based on these performance results, we quantify the ruin probability of the cyber insurer, which indicates the chance that the insurer does not have enough capital reserve to afford the claims from the outage users. Through numerical evaluation, we show that the ruin probability of the insurer can be efficiently reduced by equipping a larger number of antennas at base stations or increasing network frequency reuse.**

Index terms- Cyber insurance, cyber risk, massive MIMO, ruin theory, stochastic geometry.

I. Introduction

Securing wireless data communication has become one of the top priorities for mobile service providers due to dramatic expansion of pervasive wireless access through mobile devices over the Internet. Especially, mobile communication systems are carrying important confidential information, e.g., for financial transaction and health-care monitoring and control, through proliferating wireless services such as e-commerce, e-health-care and cloud-based applications. The loss, damage, or delay of such information can cause serious consequences to the users.

To safeguard wireless communications, physical layer security techniques [1] has emerged and caught significant research attention. It uses channel codes, e.g., Wyner codes [2], to provide direct secure communication. Thus, by focusing only on transmission parameters, physical layer security techniques avoid the use of computation resources, such as signal processing on cryptographic keys, and incur small signaling overhead. Existing efforts have mainly focused on the precoder design for multiuser downlink transmission and artificial-noise (AN)-aided jamming based on multiple-input multiple-output (MIMO) technologies [2], [3].

Although these 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. Therefore, instead of developing technological approaches to handle the cyber risks, we take a different approach by transferring the risks away from the network users via cyber insurance [4], [5]. 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 compensates indemnities to the users when damage occurs 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 [6], i.e., the chance that the insurer is unable to cover all the indemnities. The goal of the cyber insurance framework is to quantify the risks of both the insured users and insurer. To this end, we focus on investigating the user performance in a large-scale cellular network based on the stochastic geometry analysis. With the novel stochastic geometry model which is able to capture the repulsion among points, we can 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 damages occur randomly to a population of insured users, we model the stochastic claim process based on Cr´amer-Lundberg model (i.e., compound Poisson model) from collective risk theory [7]. Utilizing the analytical results for user performance, we introduce a quantitative approach to evaluate the ruin probability of the insurer.

Notations: In the following, we use $\mathbb{E}[\cdot]$ to denote coverage over all the random variables in $[\cdot]$, $\mathbb{E}_X[\cdot]$ to denote the expectation over the random variable X, and $\mathbb{P}[Z]$ to denote the probability that an event Z occurs. $\mathbf{x}_a$ denotes the location of a, and $\|\mathbf{x}_a - \mathbf{x}_b\|$ is used to represent the Euclidean norm between the coordinates $\mathbf{x}_a$ and $\mathbf{x}_b$. $\gamma(z,a) \triangleq \int_0^a \mathrm{e}^{-t} t^{z-1}\,\mathrm{d}t, z \in \mathbb{C}, a \geq 0$ denotes the lower incomplete Gamma function.

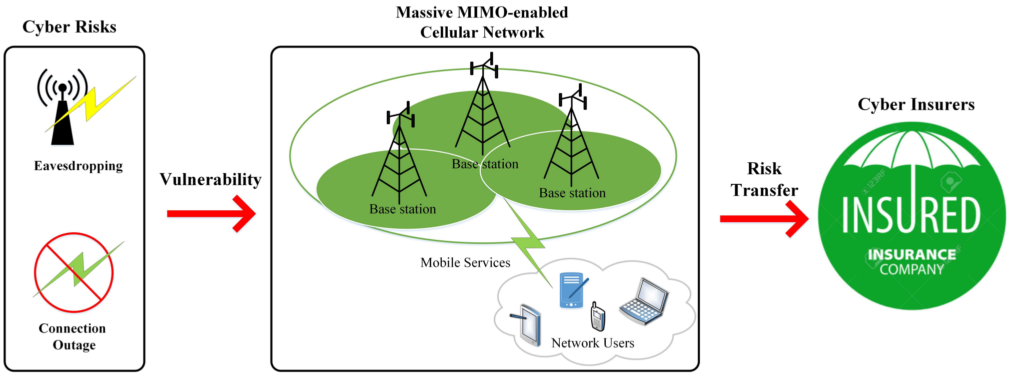


Fig. 1. Illustration of risk transfer of wireless users in the cyber insurance framework.

II. A Cyber Insurance Framework and Network Model

A. Cyber Insurance Framework

As shown in Fig. 1, 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 for an indemnity payment upon a cyber loss occurrence. For the insured, cyber insurance serves as a hedge 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.

B. Massive MIMO-enabled Cellular Network Model

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 of user adopts single antenna. Meanwhile, there exists 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 be following independent homogeneous α-Ginibre point processes (GPPs), denoted as Φ_B and Φ_E, with spatial densities ρ_B and ρ_E and repulsion factors α_B and α_E, respectively.

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 [8]. Each BS is considered to have several time-frequency resource blocks. Let N_s denote the maximum number of wireless data flows that can be supported simultaneously on each resource block. For TDD, N_s is dependent on the dimension of the uplink pilot field which decides the number of downlink channels to be estimated [9]. The BSs adopt linear zero-forcing beamforming (ZFBF) [10] with equal power per wireless downlink to serve N_s legitimate UEs simultaneously over a time-frequency resource block. As a result, Gaussian noise or uncorrelated intra-cell interference does not have effects in the massive MIMO regime (i.e., L $\gg N_s \gg 1$). For spectrum allocation of each BS, we consider frequency reuse with a factor $\xi \in (0, 1]$. The factor represents the percentage of BSs in the network that are allocated with the same spectrum frequency. For cell association, each user is served by a massive MIMO-based BS that provides the strongest *reference signal received power* [11]. This is equivalent to the nearest BS association in our considered system with homogeneous BSs. 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 flows N_s.

Let P_B denote the transmit power of the BS on each resource block and $\mathbf{x}_z$ denote the location of z. If a typical user u establishes a downlink connection with the serving BS, denoted as BS 0, its received signal-to-interference-ratio (SIR) can be calculated as follows [12]:

$$\eta_u = \frac{P_B G \beta}{N_s \|\mathbf{x}_0 - \mathbf{x}_u\|^{\mu} I_u}, \qquad (1)$$

where $G = L - N_s + 1$ represents the antenna array gain of the massive MIMO-enabled BS[1], β is a frequency dependent constant typically calculated as $\frac{3\times 10^8}{4\pi\nu}$ [13] with carrier frequency ν, and μ denotes the path-loss exponent. I_u represents the inter-cell interference given by [14]

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

where $h_{b,u} \sim \mathcal{G}(N_s, 1)$ [13] represents the channel gain between interfering BS $b \in \Phi_B$ and the typical user. Here $\mathcal{G}(a_1, a_2)$ means a gamma distribution, in which a_1 is the shape parameter and a_2 is the scale parameter.

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

$$\eta_e = \frac{P_B h_{0,e} \beta}{N_s \|\mathbf{x}_0 - \mathbf{x}_e\|^{\mu} (I_e + \sigma^2)}, \qquad (3)$$

where $h_{0,e}$ is an exponentially distributed random variable [13] representing the small-scale fading channel gain between the serving BS 0 of the typical user and an eavesdropper $e \in \Phi_E$, σ^2 is the variance of additive white Gaussian noise (AWGN), and

[1] Due to the hardening effect of a massive MIMO channel, the transmitted signals from the BS only undergo long-term effects.

I_e is the accumulated interference at e expressed as follows:

$$I_e = \sum_{b \in \Phi_B} \frac{P_B h_{b,e} \beta}{N_s \|\mathbf{x}_b - \mathbf{x}_e\|^{\mu}}, \tag{4}$$

where $h_{b,e} \sim \mathcal{G}(N_s, 1)$ [13] is the small-scale fading channel gain between the interfering BS $b \in \Phi_B$ and eavesdropper $e \in \Phi_E$.

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 [15], i.e., the eavesdropper that achieves the highest receive SINR. Additionally, we assume that the eavesdroppers' density can be estimated. This is reasonable as passive eavesdropper detection techniques, e.g., energy detection of local oscillator power leakage from the RF frontend of an eavesdropper [16], can be adopted in the network.

In this paper, we perform the analysis of the massive MIMO-enabled cellular network based on α-GPP [17] for its generosity and tractability. α-GPP is a particular type of determinantal point process 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 when κ goes to infinity. Due to its generosity and tractability, α-GPP has recently attracted much attention in network modeling [18]–[21].

III. 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. Performance Metrics

The BSs are considered to adopt the well-known Wyner's encoding scheme [2] to secure confidential information to the legitimate users. Let R_t denote the transmission rate of the codewords, which contains redundant codewords at a rate $R_e < R_t$ to safeguard the secrecy information transfer against eavesdroppers.

The wireless service provided by a BS is considered to be unsuccessful if the receive SINR at its user is lower than a target threshold τ_u. Let η denote the receive SINR at the user from its associated BS. The service outage probability of a typical user is defined as $\mathcal{P} \triangleq \mathbb{P}[\eta < \tau_u]$, where $\tau_u = 2^{R_t} - 1$.

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 receive SINR greater than $\tau_e = 2^{R_e} - 1$. Thus, the secrecy outage probability is defined as $\mathcal{O} \triangleq \mathbb{P}[\eta_{e^{\star}} > \tau_e]$.

B. Analytical Results

According to the Slivnyak's theorem [22], the analysis of user's 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 III-B 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:*

$$\begin{aligned}\mathcal{P} = 1 - 2 \int_0^R & \exp(-\pi\xi\rho_B r^2) \prod_{n\geq 0}\left(1+\alpha\frac{\gamma(n+1,\pi\xi\rho_B r^2)}{n!}\right)^{-\frac{1}{\alpha}} \\ & \times \sum_{n\geq 0}\frac{(\pi\xi\rho_B r)^{n+1} r^n}{n!}\left(1+\alpha\frac{\gamma(n+1,\pi\xi\rho_B r^2)}{n!}\right)^{-1} \\ \times \mathcal{L}^{-1} & \Bigg\{\frac{1}{s}\prod_{k\geq 0}\Bigg(1+\frac{2\alpha_B(\pi\xi\rho_B)^{k+1}}{k!}\int_r^R \exp\left(-\pi\xi\rho_B l^2\right) r^{2k+1} \\ & \times\left(1-\left(1+\frac{s\beta}{N_s l^{\mu}}\right)^{-N_s}\right)\mathrm{d}l\Bigg)^{-\frac{1}{\alpha_B}}\Bigg\}\left(\frac{\beta(L-N_s+1)}{\tau_u N_s r^{\mu}}\right)\mathrm{d}r. \end{aligned} \tag{5}$$

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

$$\begin{aligned}\mathcal{P} &= \mathbb{P}\left[\frac{P_B\beta(L-N_s+1)r_{0,u}^{-\mu}}{N_s I_u} < \tau_u\right] \\ &= \mathbb{E}_{r_{0,u}}\left[\mathbb{P}\left[\frac{I_u}{P_B} \geq \frac{\beta(L-N_s+1)}{\tau_u N_s r_{0,u}^{\mu}}\middle| r_{0,u}\right]\right] \\ &= 1 - \int_0^{\infty} F_{\frac{I_u}{P_B}|r_{0,u}}\left(\frac{\beta(L-N_s+1)}{\tau_u N_s r_{0,u}^{\mu}}\right) f_{r_{0,u}}(r)\mathrm{d}r, \end{aligned} \tag{6}$$

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 [23]

$$\begin{aligned} f_{r_{0,u}}(r) = \exp(-\pi\xi\rho_B r^2) & \prod_{n\geq 0}\left(1+\alpha\frac{\gamma(n+1,\pi\xi\rho_B r^2)}{n!}\right)^{-\frac{1}{\alpha}} \\ \times \sum_{n\geq 0} & \frac{(\pi\xi\rho_B r)^{n+1} r^n}{n!}\left(1+\alpha\frac{\gamma(n+1,\pi\xi\rho_B r^2)}{n!}\right)^{-1}. \end{aligned} \tag{7}$$

Let $\mathcal{L}_{I_u}(s) = \mathbb{E}[\exp(-sI_u)|r_{0,u}]$ denote the Laplace transform of I_u evaluated at s given $r_{0,u}$, and $\mathcal{L}^{-1}\{z\}(x)$ denote the inverse Laplace transform of z evaluated at x. By the definition of Laplace transform, the conditional CDF of $\frac{I_u}{P_B}$ can be calculated as follows:

$$\begin{aligned} & F_{\frac{I_u}{P_B}|r_{0,u}}(x) = \mathcal{L}^{-1}\left\{\frac{1}{s}\mathcal{L}_{\frac{I_u}{P_B}}(s)\right\}(x) \\ & = \mathcal{L}^{-1}\left\{\frac{1}{s}\mathbb{E}_{\Phi_B^u, h_{b,u}}\left[\exp\left(-s\sum_{b\in\Phi_B^u}\frac{h_{b,u}\beta}{N_s\|\mathbf{x}_b-\mathbf{x}_u\|^{\mu}}\right)\middle| r_{0,u}\right]\right\}(x) \\ & = \mathcal{L}^{-1}\left\{\frac{1}{s}\mathbb{E}_{\Phi_B^u}\left[\prod_{b\in\Phi_B^e}\left(1+\frac{s\beta\,\mathbb{1}\left(\|\mathbf{x}_b-\mathbf{x}_u\| > r_{0,u}\right)}{N_s\|\mathbf{x}_b-\mathbf{x}_u\|^{\mu}}\right)^{-N_s}\right]\right\}(x) \\ & \overset{\text{(a)}}{=} \mathcal{L}^{-1}\Bigg\{\frac{1}{s}\prod_{k\geq 0}\Bigg(1+\frac{2\alpha_B(\pi\xi\rho_B)^{k+1}}{k!}\int_{r_{0,u}}^R\left(1-\left(1+\frac{s\beta}{N_s l^{\mu}}\right)^{-N_s}\right) \\ & \qquad\qquad \times \exp\left(-\pi\xi\rho_B l^2\right) r^{2k+1}\mathrm{d}l\Bigg)^{-\frac{1}{\alpha_B}}\Bigg\}(x), \end{aligned} \tag{8}$$

where (a) follows by applying *[24, Lemma 3]*.

Plugging (8) and (7) into (6), we have the result in (5), which concludes the proof. □

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:*

$$\mathcal{O} = 1 - \prod_{k\geq 0}\Bigg(1+\frac{2\alpha_E(\pi\rho_E)^{k+1}}{k!}\int_0^R \prod_{k\geq 0}\Bigg(1+\frac{2\alpha_B(\pi\xi\rho_B)^{k+1}}{k!}$$
$$\times\int_0^R\Bigg(1-\Big(1+\frac{\tau_e r^{\mu}}{l^{\mu}}\Big)^{-N_s}\Bigg)\exp\left(-\pi\xi\rho_B l^2\right)l^{2k+1}\mathrm{d}l\Bigg)^{-\frac{1}{\alpha_B}}$$
$$\times\exp\Bigg(-\frac{\tau_e N_s r^{\mu}\sigma^2}{P_B\beta}-\pi\rho_E r^2\Bigg)r^{2k+1}\mathrm{d}r\Bigg)^{-\frac{1}{\alpha_E}}. \quad (9)$$

Theorem 2 can be proved following a similar approach to the proof of Theorem 1. We omit the proof of Theorem 2 here due to the space limit.

IV. Cyber-Insurance and Ruin Probability

We consider an insurer offering a cyber-insurance plan to users. The insurer can be an insurance company. Each user pays the same premium denoted by c 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 is the indemnities generated randomly from the user population given outage probabilities. The insurer is therefore interested in the ruin which is an event that its reserve, i.e., accumulated income minus accumulated indemnities, is negative. In the following, we analyze the ruin probability of the insurer [25].

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 kth claim's amount. C_k's are independent and identically-distributed. Sequence $(C_k)_{k\geq 1}$ is independent of $(N_t)_{t\in\mathbb{R}_+}$. Also, let

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

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 $c > 0$, i.e., $f(t) = ct$.

Considering cyber insurance for the users in the network introduced in Section II-B, we assume that C_k can take two values a and $a + b$ with respective probabilities p and $1 - p$. Here, p and $q := 1 - p$ denote the conditional probabilities of service outage and secrecy outage, respectively. They are defined as $p = \frac{\mathcal{P}}{\mathcal{P}+\mathcal{O}p_d}$, where $\mathcal{P}$ is the service outage probability obtained from Theorem 1, and $\mathcal{O}$ is the secrecy outage probability obtained from Theorem 2. p_d is the probability that secrecy outage causes damage to the legitimate user, 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 calculated as $\lambda = \mathcal{P} + \mathcal{O}p_d$.

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 claim process is defined as follows:

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

in which we have $S(t) = 0$ if $N_t = 0$. The surplus process $(R_y(t))_{t\geq 0}$ is defined as follows:

$$R_y(t) = y + f(t) - S(t) \quad (10)$$
$$= y + ct - \sum_{k=1}^{N_t} C_k, \qquad t \geq 0,$$

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, a formula for the finite-time ruin probability is expressed as follows [7]:

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

Let $\mathcal{M}_{[0,T]}$ denotes the lowest level of the reserve process in (10) between time 0 and some fixed time horizon $T > 0$, expressed as follows:

$$\mathcal{M}_{[0,T]} = \inf\{y + f(t) - S(t), \quad t \in [0, T]\}, \quad (11)$$

which is an explicit probabilistic representation expression for a compound Poisson process. It corresponds to the classical Crámer-Lundberg risk model that can be used for simulation purposes. Note that alternative analytical expressions for the density of $\mathcal{M}_{[0,T]}$ are also available in [26] and [27].

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

$$\psi(y, T) = \mathbb{P}\big[\mathcal{M}_{[0,T]} < -y\big], \qquad y \geq 0, \quad (12)$$

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

$$-\frac{\partial\psi}{\partial y}(y, T). \quad (13)$$

The density of $\mathcal{M}_{[0,T]}$ in (13) indicates the sensitivity of the ruin probability 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.

V. Numerical Results

In this section, we study the risk of the insurer by evaluating the ruin probability ψ in (12). The simulations are performed with the parameter setting shown in Table I unless otherwise stated.

TABLE I
PARAMETER SETTING.

Symbol	μ	P_B	ν	ρ_B	ρ_E	N_S	L	ξ	$m_{\mathcal{P}}$	$m_{\mathcal{O}}$	y	c	p_d
Value	3.5	40 dBm	1.8 GHz	5×10^{-5}	10^{-5}	20	200	0.5	3	7	10	1	1

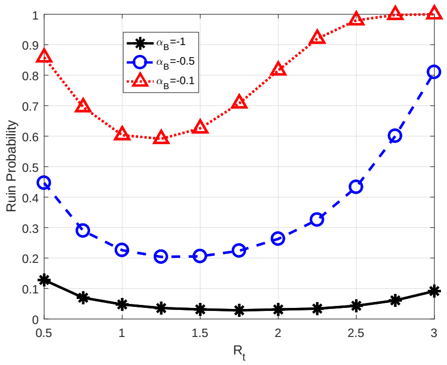


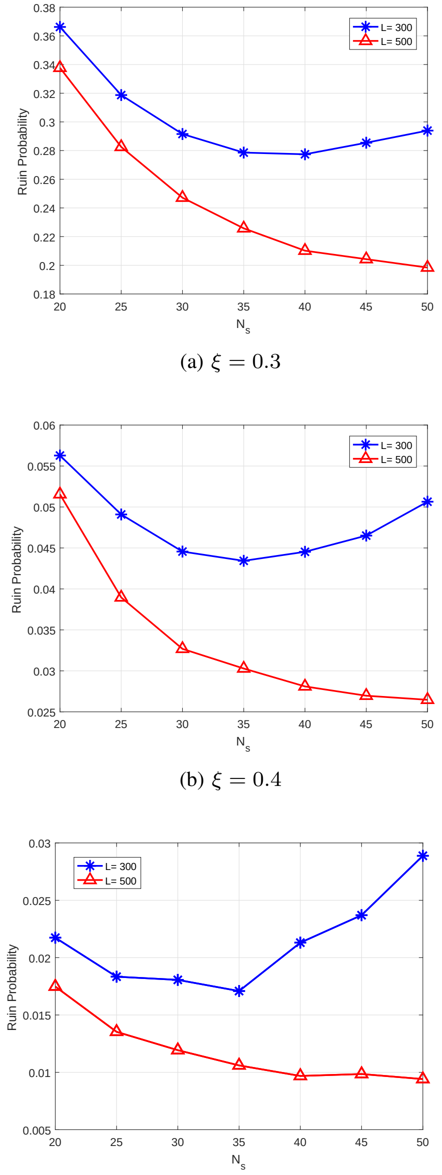
Fig. 2. Ruin probability as a function of R_t.

Additionally, the bandwidth of each resource block is 10 MHz. The noise variance is -174 dBm/Hz. The transmission rate and the redundant rate of the codewords are set at $R_t = 2$ bits/s/Hz and $R_e = 0.5R_t$, respectively.

We first focus on the influence of network parameters. Figure 2 depicts how the ruin probability varies with R_t under different α_B. We note that the ruin probability is a unimodal function of R_t. This can be intuitively understood that the increase of the code rate R_t (and thus R_e proportionally) results in larger service outage probability $\mathcal{P}$ and smaller secrecy outage probability $\mathcal{O}$. As a result, $\mathcal{P}$ and $\mathcal{O}$ result in the high ruin probability when R_t is small and large, respectively. This indicates that the ruin probability can be minimized by setting a proper code rate R_t.

Figure 3 compares the ruin probability under different frequency reuse coefficient ξ. Similar to Fig. 3, the ruin probability is also a unimodal function of N_s. Moreover, employing a larger number of antennas contributes to smaller ruin probability as the service outage probability can be mitigated. However, employing more antennas would inevitably incur a cost for the service provider. Interestingly, the ruin probability decreases with the increase of ξ. This is due to the fact that the claim size 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.

Figure 4 shows the impact of the density of eavesdroppers ρ_E on the ruin probability ψ. It can be found that ψ increases exponentially with ρ_E. This implies that increasing the density of eavesdroppers is more disruptive to the insurer when ρ_E is large than when ρ_E is small. Additionally, we observe that the ruin probability is more susceptible to α_E when the path-loss exponent is large. For example, when $\mu = 3.2$ and $\rho_E = 10^{-4}$, the difference between ψ under $\alpha_E = -1$ and that under $\alpha_E = -0.1$ is 0.82%. Such a difference is increased to 3.68% when $\mu = 3.8$.



(a) $\xi = 0.3$

(b) $\xi = 0.4$

(c) $\xi = 0.5$

Fig. 3. Ruin probability as a function of N_t.

Next, we demonstrate the effects of claim size and initial reserve on the ruin probability in Fig. 5. The claim size of a service outage $c_{\mathcal{P}}$ is fixed at 3 while that of secrecy outage $c_{\mathcal{O}}$ varies from 4 to 8. It is found that the impact of $c_{\mathcal{P}}$ on the ruin probability becomes more pronounced with the increase of $c_{\mathcal{P}}$. Additionally, it is evident that increasing the initial reserve is an effective way to lower down the ruin probability especially when the claim size 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.

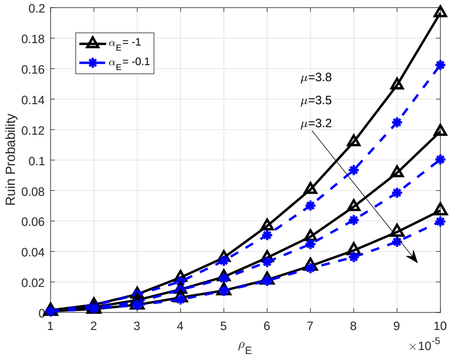


Fig. 4. Ruin probability as a function of ρ_E.

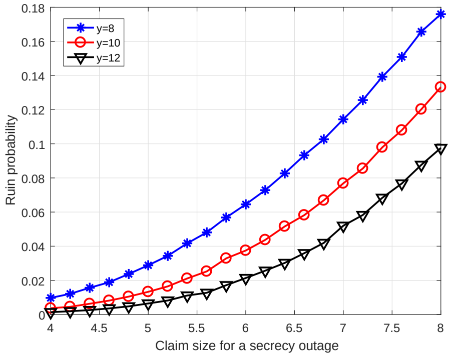


Fig. 5. Ruin probability as a function of the claim size. ($m_{\mathcal{P}} = 3$)

VI. 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 risk. Specifically, considering eavesdropping as the cyber risk, we introduce a quantitative approach to assess the vulnerabilities of an insured user 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.

VII. Acknowledgment

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada, Singapore MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15 and NRF2015-NRF-ISF001-2277, and Cyber Risk Management (CyRiM) Project by the Monetary Authority of Singapore.

References

[1] Y. S. Shiu, *et al.*, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, April 2011.

[2] A. Mukherjee, *et al.*,"Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014.

[3] X. Chen *et al.*, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027-1053, Second Quarter 2017.

[4] L. A. Gordon, P. M. Loeb, and T. Sohail, "A framework for using insurance for cyber risk management," *Communications of the ACM*, vol. 46, no. 3, pp. 81-85, March 2003.

[5] X. Lu, *et al.*,"Cyber insurance for heterogeneous wireless networks," to appear in *IEEE Communications*.

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

[7] 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.

[8] 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.

[9] Q. Ye, *et al.*, "User association and interference management in massive MIMO HetNets," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 2049-2065, May 2016.

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

[11] D. Bethanabhotla, *et al.*,"Optimal user-cell association for massive MIMO wireless networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1835-1850, March 2016.

[12] 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 Communications Letters*, vol. 19, no. 12, pp. 2294-2297, Dec. 2015.

[13] L. Wang, *et al.*, "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.

[14] 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.

[15] L. Dong, *et al.*, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[16] A. Mukherjee, and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2809-2812, March 2012.

[17] 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.

[18] X. Lu, *et al.*, "Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis," to appear in *IEEE Transactions on Wireless Communications*.

[19] I. Flint, *et al.*,"Performance analysis of ambient RF energy harvesting with repulsive point process modelling," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5402-5416, May 2015.

[20] X. Lu, *et al.*, "Self-sustainable communications with RF energy harvesting: Ginibre point process modeling and analysis," *Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1518-1535, May 2016.

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

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

[23] H. B. Kong, *et al* "Using Ginibre point processes modeling and analysis of wireless sensor networks with/without energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3700-3713, June 2017.

[24] H.-B. Kong, *et al.*,"Exact performance analysis of ambient RF energy harvesting wireless sensor networks with Ginibre point process," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3769-3784, Oct. 2016.

[25] 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.

[26] 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.

[27] 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.