

Tradeoff Between Delay and Physical Layer Security in Wireless Networks

Yi Zhong, *Member, IEEE*, Xiaohu Ge, *Senior Member, IEEE*, Tao Han, *Member, IEEE*,
Qiang Li, *Member, IEEE*, and Jing Zhang, *Member, IEEE*

Abstract—Exchange of crucial and confidential information leads to the unprecedented attention on the security problem in wireless networks. Even though the security has been studied in a number of works, the joint optimization of the physical layer security and the end-to-end delay management, which requires a meticulous cross-layer design, has seldom been evaluated. In this paper, by combining the tools from stochastic geometry and queueing theory, we analyze the tradeoff between the delay and the security performance in large wireless networks. We further propose a simple transmission mechanism which splits a message into two packets and evaluate its effect on the mean delay and the secrecy outage probability. Our numerical results reveal that the security performance is better for larger path loss exponent when the density of legitimate nodes is large, and it is reverse when the density is small. Moreover, it is observed that by introducing the simple mechanism of message split, the security performance is greatly improved in the backlogged scenario and slightly improved in the dynamic scenario when the density of legitimate transmitters is large. In summary, this paper provides an understanding and a rule-of-thumb for the practical design of wireless networks where both the delay and the security are key concerns.

Index Terms—Delay, physical layer security, Poisson point process, queueing theory, stochastic geometry.

I. INTRODUCTION

A. Motivations

THE wireless access becomes ubiquitous for the civilian and military applications [2], including the exchange of crucial and confidential information like the banking related data, leading to unprecedented attention to the security problem for the exchange of information between nodes in the wireless networks. Comparing with the traditional security methods based on the cryptographic techniques at the upper layers of the communication protocols in a wireless network [3], the physical layer security is an information-theoretic based approach that guarantees the security of wireless links by exploiting the randomness of wireless channels, which

Manuscript received September 15, 2017; revised February 1, 2018; accepted February 16, 2018. Date of publication April 11, 2018; date of current version October 18, 2018. This work was supported by the National Natural Science Foundation of China under Grant 61701183. This paper will be presented in the 2018 IEEE International Conference on Communications [1]. (*Corresponding author: Yi Zhong.*)

The authors are with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: yzhong@hust.edu.cn).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/JSAC.2018.2825798

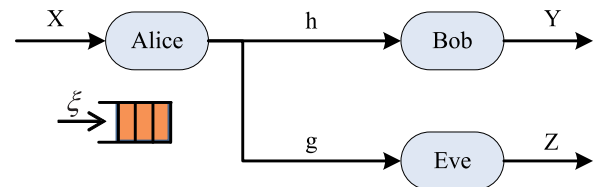


Fig. 1. Cipher system with random arrival messages: Alice attempts to deliver messages to Bob, while keeping it secret from Eve who intercepts the transmissions.

makes it more difficult for the attackers to decipher the delivered messages. From the point of view of the information theory, the security problem can be modeled by the wiretap channel proposed by Wyner in his pioneering work [4], where a source sends the information to a legitimate receiver at the presence of an eavesdropper.

On the other hand, due to the emergence of new types of latency-critical applications such as the command-and-control of drones, the advanced manufacturing, the vehicular networks [5] and the tactile Internet, the delay performance becomes an indispensable metric that should be considered in the wireless transmissions [6]. Though the delay in wireless networks has been studied by a number of works [7], [8], the joint optimization of the physical layer security and the end-to-end delay management has seldom been studied in the literature, which requires a meticulous cross-layer design. The relationship between the physical layer security and the end-to-end delay is exceedingly complex, which is affected by a number of factors, such as the random time-varying channel, the irregular deployment of nodes, the wireless transmission mechanisms and so on.

An intuitive tradeoff between the delay and the physical layer security could be observed from Figure 1, where a transmitter named Alice attempts to deliver messages to a legitimate receiver named Bob, while keeping it secret from an eavesdropper named Eve who intercepts the transmissions. Alice maintains a buffer of infinite capacity to store the incoming packets, and the time is divided into discrete slots with equal duration. In each time slot, Alice attempts to transmit its head-of-line packet with a certain probability p if its buffer is not empty. A failure occurs if Bob cannot decode the packets sent by Alice. When a failure occurs, Alice retransmits the packet in the next time slot with the same access probability p . The security constraint is that the probability of a packet delivered by Alice failing to achieve perfect secrecy from the detrimental eavesdropper Eve is

less than certain threshold. Increasing the transmit power of Alice reduces the delay but makes it more easier for Eve to decode the message, thus decreasing the security as well. Moreover, in wireless networks with multiple legitimate links and multiple eavesdroppers, the tradeoff between the delay and the physical layer security is much more perplexed. For example, increasing the transmit probability p may decrease the delay for legitimate links and increase the chance for Eve to intercept the messages since the probability to schedule the packets is increased, but it also increases the interference in wireless networks which makes it harder for Eve to intercept the messages.

The motivation of this work is to evaluate the tradeoff between the delay and the physical layer security in wireless networks. Particularly, we model the spatial distribution of legitimate nodes and eavesdroppers in wireless networks by using the tools from the point process theory. Through combining the point process theory and the queueing theory, we analyze the tradeoff between the delay and the physical layer security theoretically. Our work will provide a useful guideline for the design of secure wireless transmissions while meeting the end-to-end delay requirements imposed by the mobile applications in wireless networks.

B. Related Works

The work in [9] extends the Wyner's wiretap channel model [4] to the case of broadcast channels with confidential messages, which shows that perfect secrecy could be achieved if the legitimate link has a better channel than the link of eavesdropper. The work in [10] demonstrates that the secrecy capacity, i.e., the maximum achievable rate of the legitimate link while guaranteeing that the eavesdropper cannot decode the message, is the difference of the maximum achievable rates between the legitimate link and the eavesdropping link.

Most of the studies on physical layer security in the literature focused on the scenes of a small number of nodes. For instance, the works in [11] and [12] studied the security problem in the case of a small number of nodes with multiple antennas, and the works in [13]–[15] studied the security problem in the cooperative transmission and in the multiple access channels. The works in [16] and [17] studied the secure and reliable transmission for the multiple-input multiple-output systems. Recently, due to the applications of stochastic geometry tools in the wireless networks [18], a few studies have been carried out to analyze the security problem in large wireless networks. For example, the works in [19]–[22] studied the connectivity problem in the wireless network where the legitimate nodes and the eavesdroppers are randomly distributed in space, and the works in [23]–[25] evaluated the coverage and the capacity with the limitation of security. The work in [26] studied the information-theoretic secrecy performance in large cellular networks by modeling the locations of both base stations and mobile users as two independent Poisson point processes (PPP) [27]–[31]. The work in [32] studies the throughput of large decentralized wireless networks with physical layer security constraints, and

the authors also utilize the tools from stochastic geometry to model the wireless networks.

Though the relationship between the security and the capacity of large wireless networks has been well explored in the literature, few works have been done to evaluate the relationship between the security and the delay in large wireless networks. Part of the reason is that the analysis of delay in large wireless network is far more difficult than the analysis of coverage and capacity since the delay is a complicated function of all links and is affected by an unusually large number of variables such as the network load, the medium access protocol, the path loss, and so on. In [33], the joint optimization of the physical layer security and the end-to-end delay is studied in the wireless body area networks. In [34], the resource allocation problem is studied in the cognitive radio network with delay and security constraints. However, these works considers few nodes in the network and have not obtained the analytical results for the large wireless networks. Recently, several tentative works appear to analyze the delay in large scale wireless networks, such as [35]. The basic idea is to combine the stochastic geometry and the queueing theory, which results in the challenge of interacting queues problem [36]–[38], i.e., the service rates of the queues in the networks rely on the status of all queues in the networks. Our previous works have derived the conditions for the stability of queues [39] and the bounds for the delay [7] in large wireless networks.

C. Contributions

In this work, we evaluate the tradeoff between the delay and the security performance in large wireless networks for both the backlogged scenario and the dynamic scenario. To our best knowledge, this is the first work to explore the joint optimization of the delay and the security problem in large wireless networks. By combining the tools from stochastic geometry and queueing theory, we introduce some new analytical approaches and derive the close-formed results for the mean delay and the secrecy outage probability (i.e., the probability of a transmission failing to achieve perfect secrecy). We also propose a simple transmission mechanism which splits a message into two packets and analyze its effect on the delay and security performance.

Based on the numerical results, we find that the security performance of a large wireless network is better for larger path loss exponent when the density of legitimate nodes is large, and it is reverse when the density is small. We also find that under the condition that a certain confidential rate (i.e., the achievable rate of confidential messages with the constraint of perfect secrecy) is guaranteed, the delay performance is better in high signal-to-interference ratio (SIR) regime than that in low SIR regime. By introducing the simple mechanism of message split, it is shown that the delay performance in the backlogged scenario is improved when the density of legitimate transmitters is large. Meanwhile, introducing message split greatly improves the security performance in the backlogged scenario, while slightly improves the security performance in the dynamic scenario for small density of legitimate nodes.

To sum up, our contributions in this work could be summarized as follows.

- The joint optimization of the delay and the security problem in large wireless networks, which is seldom explored in the literature, is evaluated through numerical analysis.
- New analytical approaches based on the combination of stochastic geometry and queueing theory are proposed to derive the mean delay and the secrecy outage probability in the scenario of random traffic.
- Numerical evaluation based on the theoretical analysis is conducted to gain insight for the practical design of wireless networks where both the delay and the security are key concerns.

The remaining part of the paper is organized as follows. Section II describes the propagation model, the traffic model, and the secrecy transmission rate. Section III analyzes the delay in two different scenarios respectively, i.e., the backlogged scenario and the dynamic scenario. Section IV proposes and analyzes a simple transmission mechanism, in which a confidential message is divided into two packets to be delivered independently. Section V numerically analyzes the tradeoff between the security and the delay performance. Finally, Section VI concludes the paper.

II. SYSTEM MODEL

We consider an ad hoc network consisting of both legitimate nodes and eavesdroppers in a large two-dimensional space. The locations of the legitimate transmitters are modeled as a homogeneous PPP Φ_l with intensity λ_l , and the locations of the eavesdroppers are modeled as another independent homogeneous PPP Φ_e with intensity λ_e . Each legitimate transmitter is paired with a legitimate receiver at a fixed distance r_0 and a random orientation. Without loss of generality, we consider a typical legitimate transmitter located at the origin, and the corresponding legitimate receiver is located at x_0 with $|x_0| = r_0$ (see Fig. 2). We consider the discrete time system where the time is divided into discrete slots with equal duration, and each transmission attempt occupies exactly one time slot. In practice, the locations of the transmitters and the receivers are generated once at the beginning and then kept unchanged during all time slots. Therefore, the topology of the network could be considered as static.

A. Propagation Model

The propagation model in this work consists of two parts, i.e., the path loss and the fading. We assume that the standard power path loss model is used, and the average received power at a receiver y from a transmitter x is denoted by

$$P_r = P_t|x - y|^{-\alpha}, \tag{1}$$

where P_t is the transmit power, P_r is the received power, and α is the path loss exponent ($\alpha \geq 2$). The fading of each link is assumed to be Rayleigh block fading with zero mean and unit variance, and it is independent between different links. The power fading coefficients in different time slots

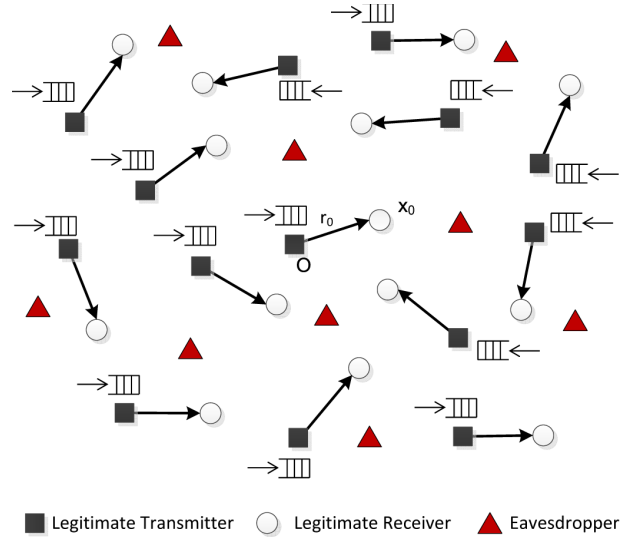


Fig. 2. Topology of the network, where the squares denotes the legitimate transmitters, the circles denote the legitimate receivers and the triangles denote the eavesdroppers.

are independent identically distributed (i.i.d.) and are constant during one time slot. Note that the channel model in our work is not as comprehensive as that in [40] which considers the path loss, the Rayleigh fading, the azimuth angle of departure and the log-normal shadowing. However, the channel model in our work is a common assumption that has been widely accepted in the literatures, such as [41]. Meanwhile, using the model of the path loss and the Rayleigh block fading may greatly reduce the complexity of the derivations and make the analysis tractable, and close-form results could be obtain to gain intuitive insight. Due to the fact that most of the existing wireless networks are interference-limited, i.e., the noise is much smaller compared with the interference, we ignored the thermal noise in our analysis. Without loss of generality, the transmit power of all legitimate transmitters is normalized.

When all transmitters are active, the SIR at the typical legitimate receiver x_0 is

$$SIR_{x_0} = \frac{h_{x_0}r_0^{-\alpha}}{\sum_{y \in \Phi_l} h_y|y - x_0|^{-\alpha}}, \tag{2}$$

where h_{x_0} is the fading coefficient between the typical legitimate transmitter at the origin and the corresponding receiver at x_0 , $\{h_y\}$ is the fading coefficients between the transmitter $y \in \Phi_l$ and the typical legitimate receiver x_0 .

When all transmitters are active, the SIR at an eavesdropper $x_e \in \Phi_e$ is

$$SIR_{x_e} = \frac{h_e|x_e|^{-\alpha}}{\sum_{y \in \Phi_l} h_y|y - x_e|^{-\alpha}}, \tag{3}$$

where h_e is the fading coefficient between the legitimate transmitter at the origin and the eavesdropper at x_e .

B. Traffic Model

For completeness consideration, we consider two scenarios for the traffic arrival process, i.e., *the backlogged scenario* and *the dynamic scenario* (see Figure 3).

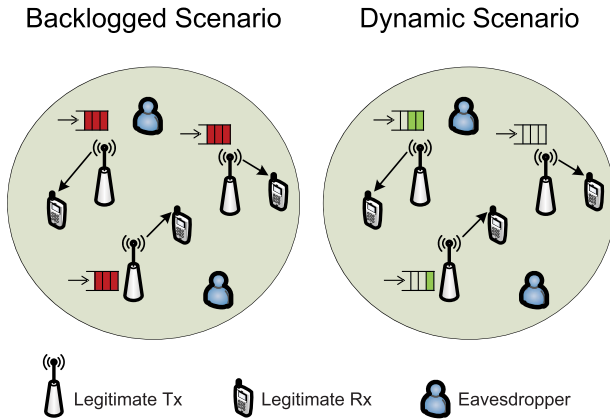


Fig. 3. Two scenarios for the traffic arrival process, i.e., the backlogged scenario and the dynamic scenario.

1) *Backlogged scenario*: In the backlogged scenario, we assume that the network is backlogged, i.e., the transmitters always have packets to transmit when they are scheduled for transmission. In this way, a meaningful and practically relevant metric in the backlogged scenario is the duration to successfully deliver one packet, which is closely related to the number of retransmissions of a packet. This type of delay, which ignores the queuing delay (i.e., the waiting time of a packet until it is served), is also defined as local delay [40]–[42]. Without loss of generality, we call it the delay for simplicity in the backlogged scenario.

2) *Dynamic scenario*: In the dynamic scenario, we assume that the packets arrive at the legitimate transmitters as a stochastic process. The packets arrival process at each legitimate transmitter $x_i \in \Phi_t$ is assumed to be an independent Bernoulli process of arrival rate ξ per time slot. By the definition of the Bernoulli process, ξ is the probability of an arrival of a packet at user x_i in any time slot.

We assume that each legitimate transmitter maintains a buffer with infinite capacity to store the incoming packets. In each time slot, each legitimate transmitter attempts to transmit its head-of-line packet with probability p if the queue at the transmitter is not empty. As for the retransmission mechanism, we assume that if a packet fails for transmission in the scheduled time slot, the packet will be added into the head of the queue of the corresponding legitimate transmitter and wait to be rescheduled again.

C. Secrecy Transmission Rate

According to Wyner's secure encoding scheme [4], [42], a transmitter may choose two rate thresholds, i.e., the rate threshold of codewords R_t and the rate threshold of confidential messages R_s . The difference between the two rate thresholds, denoted by $R_e = R_t - R_s$, is the rate cost of securing the messages against eavesdropper. If the rate of a legitimate link is less than the threshold R_t , the legitimate receiver cannot decode the message with an arbitrarily small error. Meanwhile, if the rate of every eavesdropping link is less than the threshold R_e , perfect secrecy could be achieved to guarantee the confidential rate R_s .

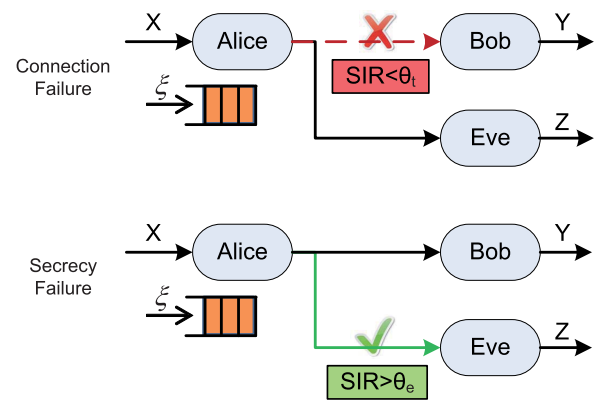


Fig. 4. Two failure events for a transmission attempt, i.e., the connection failure and the secrecy failure.

With the above two rate thresholds, we define two failure events for a transmission attempt, i.e., the connection failure and the secrecy failure (see Figure 4).

1) *Connection Failure*: The connection failure means that a transmission attempt of a packet sent by a legitimate transmitter cannot be successfully decoded by the corresponding receiver. The probability of connection failure for a transmission attempt is

$$\begin{aligned} \mathcal{P}_{cf} &= \mathbb{P}\{\log_2(1 + \text{SIR}_{x_0}) < R_t\} \\ &= \mathbb{P}\{\text{SIR}_{x_0} < 2^{R_t} - 1\}. \end{aligned} \quad (4)$$

Let $\theta_t = 2^{R_t} - 1$ be the SIR threshold for the connection failure event. Due to the retransmission mechanism, if a transmission attempt of a packet fails, the packet will be added into the head of the queue and wait to be rescheduled for transmission.

2) *Secrecy Failure*: The secrecy failure means that a transmission attempt of a packet sent by a legitimate transmitter is not perfectly secure against the eavesdroppers. The probability of secrecy failure for a transmission attempt is

$$\begin{aligned} \mathcal{P}_{sf} &= 1 - \prod_{x_e \in \Phi_e} \mathbb{P}\{\log_2(1 + \text{SIR}_{x_e}) < R_e\} \\ &= 1 - \prod_{x_e \in \Phi_e} \mathbb{P}\{\text{SIR}_{x_e} < 2^{R_e} - 1\}. \end{aligned} \quad (5)$$

Let $\theta_e = 2^{R_e} - 1$ be the SIR threshold for the secrecy failure event. Since a packet may be retransmitted for several times due to the connection failure, the delivery of a packet is perfectly secure only when all the transmission attempts are successful.

Therefore, the delay in the backlogged scenario is the number of time slots required by a legitimate transmitter to successfully deliver a packet to the corresponding legitimate receiver. On the other hand, the delay in the dynamic scenario is the number of time slots between the arrival of a packet and the successful delivery of that packet. Meanwhile, the secrecy performance can be characterized by the secrecy outage probability, which in this paper is defined as the probability that at least one transmission attempt of a packet is not perfectly secure. Let N_r be the total number of scheduled transmissions until a packet is successfully decoded at the legitimate receiver, and N_r is a geometric distributed random variable with success

probability $1 - \mathcal{P}_{cf}$, i.e., $N_r \sim \text{Geo}(1 - \mathcal{P}_{cf})$. Then, the secrecy outage probability with given N_r is

$$\mathcal{P}_{so} = 1 - (1 - \mathcal{P}_{sf})^{N_r}. \quad (6)$$

The relationship between the mean delay and the secrecy outage probability is not straightforward. Intuitively, the equation (6) reveals that increasing the total number of transmissions N_r raises the mean delay as well as the secrecy outage probability. However, since the probability of secrecy failure \mathcal{P}_{sf} may decrease, the secrecy outage probability may also decrease. Therefore, the theoretical analysis of the mean delay and the secrecy outage probability is necessary. In the following discussions, we derive the expressions to reveal the exact relationship between the mean delay and the secrecy outage probability.

The system model described above is a general mathematical framework that could be applied to analyze the security and delay performance of general large wireless networks, corresponding to a number of application scenarios. For example, the proposed mathematical framework could be applied in the military communications, where the soldiers from one army want to eavesdrop the confidential messages from the hostile army. In this application scenario, the soldiers from the eavesdropping army could be considered as eavesdroppers and the soldiers from the other army could be considered as the legitimate nodes. Another application scenario could be the prevention of theft in the wireless banking transactions, where the thieves could be considered as the eavesdroppers and the banking users could be considered as the legitimate nodes. In these application scenarios, all eavesdroppers try to eavesdrop the confidential messages from all legitimate users. Thus, the legitimate users should prevent their confidential messages from being eavesdropped by any one of the eavesdroppers.

III. DELAY AND SECRECY OUTAGE PROBABILITY

The delay in the backlogged scenario is exactly the transmission delay caused by retransmission (i.e., the time to successfully transmit a packet that is served), while the delay in the dynamic scenario consists of two parts, i.e., the queuing delay and the transmission delay. We analyze the delay in the two different scenarios respectively in the following discussions.

A. Backlogged Scenario

In the backlogged scenario, whenever a transmitter is scheduled to access the channel it always has packet to transmit. The backlogged assumption is widely used in the analysis of wireless communication systems. With the backlogged assumption, the obtained interference in the network is an upper bound for the interference without backlogged assumption. Therefore, the performance derived with the backlogged assumption will be a useful bound for the performance of the practical system. With the backlogged assumption, considering the queuing delay is meaningless since the queuing delay is always infinite. However, a meaningful and practically relevant metric in the backlogged scenario is the transmission delay. The transmission delay in the backlogged scenario is exactly the local delay, which has been well explored in the

literature, such as [41] and [43]. Another benefit of introducing the backlogged assumption is that the theoretical analysis of delay becomes tractable since the interacting between different queues is avoided. Concise and close-formed results could be obtained by the backlogged assumption, which further leads to more insights. From [41], we get the following lemma, which gives the analytical expression for the mean delay of the typical legitimate link.

Theorem 1: The mean delay of the typical legitimate link in the backlogged scenario is

$$\mathcal{D} = \frac{1}{p} \exp(\lambda_l \pi r_0^2 \theta_t^\delta C(\delta) p (1-p)^{\delta-1}), \quad (7)$$

where $\theta_t = 2^{R_t} - 1$, $\delta = 2/\alpha$ and $C(\delta) = \Gamma(1+\delta)\Gamma(1-\delta) = 1/\text{sinc}(\delta)$.

Proof: The proof is ignored in this paper for conciseness since it is similar to the proof in [41, Lemma 2] and [43, Th. 3]. \square

The result in Theorem 1 is closed-form and can be easily evaluated, and it shows directly how the mean delay varies with the transmit probability p . The equation (7) indicates that the mean delay goes to infinite both when p decreases to zero and when p increases to one since $\delta < 1$ holds. When the transmit probability p decreases to zero, a packet is scheduled for transmission for very small probability, and when the transmit probability p increases to one, the interference and the interference correlation may greatly deteriorate the delay performance.

In the following, we derive the secrecy outage probability for the backlogged scenario. Note that N_r is the total number of transmissions until a packet is successfully decoded at the legitimate receiver. Then, Theorem 1 gives the analytical expression for the mean times of transmissions $\mathbb{E}\{N_r\} = \mathcal{D}$ in the backlogged scenario. For the typical legitimate link, when the realization of Φ_l is given, the connection failure probability is determined by the fading and random access mechanism, which are independent among different time slots. Thus, the connection failure probability with given Φ_l , denoted by $\mathcal{P}_{cf}^{\Phi_l}$, is the same for all time slots. Let $N_r^{\Phi_l}$ be the total number of transmissions until a packet is successfully decoded at the legitimate receiver when Φ_l is given. Then, $N_r^{\Phi_l}$ is a geometric distributed random variable with success probability $\mathcal{P}_{cf}^{\Phi_l}$, i.e., $N_r^{\Phi_l} \sim \text{Geo}(1 - \mathcal{P}_{cf}^{\Phi_l})$. In order to guarantee the perfect secrecy, each of the $N_r^{\Phi_l}$ transmission attempts should be perfect secure; otherwise, the message will be eavesdropped. Letting $\mathcal{P}_{sf}^{\Phi_l, \Phi_e}$ be the secrecy failure probability with given Φ_l and Φ_e , the secrecy outage probability is

$$\begin{aligned} \mathcal{P}_{so} &= 1 - \mathbb{E}_{\Phi_l, \Phi_e} [(1 - \mathcal{P}_{sf}^{\Phi_l, \Phi_e})^{N_r^{\Phi_l}}] \\ &= 1 - \mathbb{E}_{\Phi_l, \Phi_e} \left[\sum_{n=1}^{\infty} (1 - \mathcal{P}_{sf}^{\Phi_l, \Phi_e})^n \mathbb{P}\{N_r^{\Phi_l} = n\} \right] \\ &\stackrel{(a)}{=} 1 - \mathbb{E}_{\Phi_l, \Phi_e} \left[\sum_{n=1}^{\infty} (1 - \mathcal{P}_{sf}^{\Phi_l, \Phi_e})^n (1 - \mathcal{P}_{cf}^{\Phi_l}) (\mathcal{P}_{cf}^{\Phi_l})^{n-1} \right] \\ &= 1 - \mathbb{E}_{\Phi_l, \Phi_e} \left[\frac{1 - \mathcal{P}_{cf}^{\Phi_l}}{\mathcal{P}_{cf}^{\Phi_l}} \sum_{n=1}^{\infty} \left((1 - \mathcal{P}_{sf}^{\Phi_l, \Phi_e}) \mathcal{P}_{cf}^{\Phi_l} \right)^n \right] \\ &= \mathbb{E}_{\Phi_l, \Phi_e} \left[\frac{\mathcal{P}_{sf}^{\Phi_l, \Phi_e}}{1 - \mathcal{P}_{cf}^{\Phi_l} + \mathcal{P}_{sf}^{\Phi_l, \Phi_e} \mathcal{P}_{cf}^{\Phi_l}} \right], \quad (8) \end{aligned}$$

where (a) holds since $N_r^{\Phi_l}$ is a geometric distributed random variable with success probability $1 - \mathcal{P}_{cf}$. The last equation holds due to the sum formula of infinite geometric series whose successive terms have a common ratio. With the above discussion, we could further derive the secrecy outage probability in the following theorem.

Theorem 2: The secrecy outage probability of the typical link in the backlogged scenario can be approximated by

$$\mathcal{P}_{so} \simeq \frac{\exp\left(\frac{\lambda_e}{p\lambda_l\theta_t^2 C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{p\lambda_l\theta_t^2 C(\delta)}\right) + \exp(-p\lambda_l\pi r_0^2\theta_t^2 C(\delta)) - 1}. \quad (9)$$

Proof: See Appendix A. \square

The secrecy outage probability given by Theorem 2 is closed-form, and the relationship between the secrecy outage probability and the system parameters can be observed directly from the equation (9). The equation (9) also verifies the intuition that the secrecy outage probability is positively correlated with the intensity of the eavesdroppers λ_e and is negative correlated with the intensity of the legitimate transmitters λ_l . Specially, we get $\mathcal{P}_{so} \rightarrow 0$ as $\lambda_e \rightarrow 0$, and $\mathcal{P}_{so} \rightarrow 1$ as $\lambda_e \rightarrow +\infty$. The reason is that increasing the intensity of eavesdroppers may increase the probability that an eavesdropper appears nearby the legitimate links. Meanwhile, increasing the intensity of legitimate transmitters may increase the interference in the wireless network, thus preventing the message from being eavesdropped. Note that when either $p \rightarrow 0$ or $\lambda_l \rightarrow 0$ holds, the secrecy outage probability goes to one, i.e., $\mathcal{P}_{so} \rightarrow 1$, indicating that the secrecy outage event happens with high probability when there are very few active legitimate transmitters. This observation illustrates that increasing the number of concurrent transmissions in the wireless networks is helpful to improve the secrecy performance, i.e., increasing the interference in the wireless networks is helpful from the aspect of the security performance.

B. Dynamic Scenario

In the dynamic scenario, the delay consists of the queueing delay and the transmission delay. The analysis of the delay in the dynamic scenario requires the combination of the stochastic geometry and the queueing theory, which induces the interacting queues problem. In order to bypass these difficulties, we propose an approach to approximate the delay in the dynamic scenario. We first simplify the interaction between the queues and assume that all interfering transmitters are active with the same probability q . Then, we derive the connection failure probability \mathcal{P}_{cf} for the typical legitimate link in each time slot. The service rate of the queue at the typical legitimate transmitter will be $p(1 - \mathcal{P}_{cf})$, which means that the probability for a packet at the typical user being scheduled and successfully transmitted in a time slot is $p(1 - \mathcal{P}_{cf})$. Then, $\rho = \frac{\xi}{p(1 - \mathcal{P}_{cf})}$ represents the average proportion of time occupied by a transmitter. When the queue is empty, the transmitter is inactive, and when the transmitter is occupied, it is active with probability p due to the random access. Therefore, the active probability of the typical legitimate link is $\min\{p\rho, 1\} = \min\left\{\frac{\xi}{1 - \mathcal{P}_{cf}}, 1\right\}$. Note that \mathcal{P}_{cf} is

a function of q . By solving the equation $\min\left\{\frac{\xi}{1 - \mathcal{P}_{cf}}, 1\right\} = q$, we obtain a solution $q = q^*$ which could be used to derive the approximated delay for the wireless network.

Since the transmissions of the typical user in different time slots are affected by the independent fading and the independent random access, the probability for a transmission attempt to be scheduled and successful in all time slots is the same, which is $p(1 - \mathcal{P}_{cf})$. Therefore, the queueing system at the typical transmitter is a Geo/G/1 queue, or a discrete-time single server retrial queue [44], [45]. In the Geo/G/1 queue, the arrival process of the packets is a Bernoulli process with intensity ξ packets per time slot. The arrival process of the packets is called the geometric arrival since the probability that a packet arrives in a time slot is ξ , and the number of time slots between two adjacent arrivals is a geometric random variable. The success probability is $p(1 - \mathcal{P}_{cf})$ and the service times of packets are i.i.d. with geometric distribution. From [44], we get the mean delay \mathcal{D} for the Geo/G/1 queue with given \mathcal{P}_{cf} as

$$\mathcal{D} = \begin{cases} \frac{1 - \xi}{p(1 - \mathcal{P}_{cf}) - \xi} & \text{if } p(1 - \mathcal{P}_{cf}) > \xi \\ \infty & \text{if } p(1 - \mathcal{P}_{cf}) \leq \xi. \end{cases} \quad (10)$$

With the above discussions, we could obtain the mean delay in the dynamic scenario in the following theorem.

Theorem 3: The mean delay of the typical legitimate link in the dynamic scenario is

$$\mathcal{D} \simeq \frac{1 - 1/\xi}{1 + \frac{p\lambda_l\pi r_0^2\theta_t^2 C(\delta)}{\mathcal{W}(-\xi\lambda_l\pi r_0^2\theta_t^2 C(\delta))}}. \quad (11)$$

Proof: By assuming that all interfering transmitters are active with the same probability q , we get the connection failure probability as

$$\begin{aligned} \mathcal{P}_{cf} &= 1 - \mathbb{E}_{\Phi_l} \left[\prod_{y \in \Phi_l} \left(\frac{q}{1 + \theta_t r_0^\alpha |y|^{-\alpha}} + 1 - q \right) \right] \\ &= 1 - \exp(-q\lambda_l\pi r_0^2\theta_t^2 C(\delta)). \end{aligned} \quad (12)$$

Considering the equation $\min\left\{\frac{\xi}{1 - \mathcal{P}_{cf}}, 1\right\} = q$, we get

$$\min \left\{ \frac{\xi}{\exp(-q\lambda_l\pi r_0^2\theta_t^2 C(\delta))}, 1 \right\} = q. \quad (13)$$

Solving the above equation, we get the solution

$$q^* = \min \left\{ -\frac{\mathcal{W}(-\xi\lambda_l\pi r_0^2\theta_t^2 C(\delta))}{\lambda_l\pi r_0^2\theta_t^2 C(\delta)}, 1 \right\}. \quad (14)$$

where $\mathcal{W}(z)$ is the Lambert- \mathcal{W} function with the defining equation $\mathcal{W}(z)\exp(\mathcal{W}(z)) = z$. Then, the connection failure probability is

$$\begin{aligned} \mathcal{P}_{cf} &= 1 - \frac{\xi}{q^*} \\ &= \min \left\{ 1 + \frac{\xi\lambda_l\pi r_0^2\theta_t^2 C(\delta)}{\mathcal{W}(-\xi\lambda_l\pi r_0^2\theta_t^2 C(\delta))}, 1 - \xi \right\}. \end{aligned} \quad (15)$$

Having derived the connection failure probability, the mean delay is

$$\begin{aligned} \mathcal{D} &= \frac{1 - \xi}{p(1 - \mathcal{P}_{cf}) - \xi} \\ &= \frac{1 - 1/\xi}{1 + \frac{p\lambda_l\pi r_0^2\theta_t^2 C(\delta)}{\mathcal{W}(-\xi\lambda_l\pi r_0^2\theta_t^2 C(\delta))}}. \end{aligned} \quad (16)$$

Therefore, we get the results in the theorem. \square

It is hard to interpret the relationship between the mean delay and the system parameters since the property of the Lambert- \mathcal{W} function is not intuitive. However, we could further simplify the above results for some special cases. Note that when $x \rightarrow 0$, the asymptotic expansions of the Lambert- \mathcal{W} function is

$$\begin{aligned} \mathcal{W}(x) &= \sum_{n=1}^{\infty} \frac{(-n)^{n-1}}{n!} x^n \\ &= x - x^2 + \frac{3}{2}x^3 - \frac{8}{3}x^4 + \dots \end{aligned} \quad (17)$$

Therefore, we have $\mathcal{W}(x) \sim x$ when $x \rightarrow 0$. When $\lambda_l r_0^2 \theta_t^\delta C(\delta) \rightarrow 0$, the result given by Theorem 3 can be simplified into

$$\begin{aligned} \mathcal{D} &\simeq \frac{1 - 1/\xi}{1 + \frac{p\lambda_l \pi r_0^2 \theta_t^\delta C(\delta)}{\mathcal{W}(-\xi \lambda_l \pi r_0^2 \theta_t^\delta C(\delta))}} \\ &\simeq \frac{1 - 1/\xi}{1 - p/\xi} \end{aligned} \quad (18)$$

The above result indicates that when either $\lambda_l \rightarrow 0$, $r_0 \rightarrow 0$, or $\theta_t \rightarrow 0$ holds, the delay could be approximated into simple form. Then, the relationship between the mean delay \mathcal{D} , the transmit probability p and the arrival rate ξ could be easily obtained.

The secrecy failure event happens in the transmitting process and is not affected by the queueing process. Thus, the secrecy outage probability in the dynamic scenario is similar to that in the backlogged scenario since the secrecy outage is only determined by the delivering process of a packet. The only difference between the secrecy outage probability in the backlogged scenario and that in the dynamic scenario is that the active probabilities for the two scenarios are different. In the backlogged scenario, the active probability for the interfering transmitters is the transmit probability p since all transmitters are backlogged and always have packets to transmit. However, in the dynamic scenario, the active probability is q^* . Therefore, we get the following theorem, which gives the secrecy outage probability in the dynamic scenario.

Theorem 4: The secrecy outage probability of the typical link in the dynamic scenario can be approximated by

$$\mathcal{P}_{\text{so}} \simeq \frac{\exp\left(\frac{\lambda_e}{q^* \lambda_l \theta_e^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{q^* \lambda_l \theta_e^\delta C(\delta)}\right) + \exp\left(-q^* \lambda_l \pi r_0^2 \theta_t^\delta C(\delta)\right) - 1}, \quad (19)$$

where q^* is given by

$$q^* = \min \left\{ -\frac{\mathcal{W}(-\xi \lambda_l \pi r_0^2 \theta_t^\delta C(\delta))}{\lambda_l \pi r_0^2 \theta_t^\delta C(\delta)}, 1 \right\}. \quad (20)$$

Proof: The proof is similar to that of Theorem 2. \square

The equation (19) shows that $\mathcal{P}_{\text{so}} \simeq 0$ as $\lambda_e \rightarrow 0$ or $\theta_e \rightarrow \infty$, indicating that when the number of eavesdroppers is very small or when the SIR threshold to eavesdrop the message is very large, the secrecy outage event hardly ever happens. On the other hand, when $\lambda_e \rightarrow \infty$ or $\theta_e \rightarrow 0$, we get $\mathcal{P}_{\text{so}} \simeq 1$, indicating that when the eavesdroppers are densely deployed or when the messages are easily intercepted

by the eavesdroppers, the secrecy outage event almost always happens.

Similar to the discussions after Theorem 3, we can also simplify the result given by Theorem 4. Note that $\mathcal{W}(x) \sim x$ as $x \rightarrow 0$. When $r_0^2 \theta_t^\delta C(\delta) \rightarrow 0$, the active probability given by the equation (20) can be simplified as

$$q^* = \min\{\xi, 1\}. \quad (21)$$

Note that if $\xi > 1$, the arrival rate is larger than the transmit probability, thus, the queues in the network will be unstable. A more relevant case is $\xi < 1$, which is a necessary condition for the queues to be stable. If both $r_0^2 \theta_t^\delta C(\delta) \rightarrow 0$ and $\xi < 1$ hold, the active probability will be

$$q^* = \xi. \quad (22)$$

Plugging $q^* = \xi$ into (19), we get the secrecy outage probability when $r_0^2 \theta_t^\delta C(\delta) \rightarrow 0$ as

$$\begin{aligned} \mathcal{P}_{\text{so}} &\simeq \frac{\exp\left(\frac{\lambda_e}{\xi \lambda_l \theta_e^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{\xi \lambda_l \theta_e^\delta C(\delta)}\right) + \exp\left(-\xi \lambda_l \pi r_0^2 \theta_t^\delta C(\delta)\right) - 1} \\ &\simeq \frac{\exp\left(\frac{\lambda_e}{\xi \lambda_l \theta_e^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{\xi \lambda_l \theta_e^\delta C(\delta)}\right)} \\ &= 1 - \exp\left(-\frac{\lambda_e}{\xi \lambda_l \theta_e^\delta C(\delta)}\right). \end{aligned} \quad (23)$$

The relationship between the secrecy outage probability and the system parameters, such as the intensity of eavesdroppers λ_e , the intensity of legitimate transmitters λ_l , the SIR threshold θ_e and so on, could be observed from the equation (23) directly.

IV. PERFORMANCE OF MESSAGE SPLIT

In this section, we propose and analyze a simple transmission mechanism, in which a confidential message is divided into two packets to be delivered independently. A confidential message is successfully decoded at the legitimate receiver only when both of the two packets from the message are successfully decoded at the receiver. Meanwhile, the perfect security could be guaranteed if at least one of the two packets from the same message cannot be decoded by an eavesdropper. This transmission mechanism has a direct effect on the delay of the network and may also affect the security performance. Therefore, in this section, we explore this simple transmission mechanism to provide a guidance to tradeoff the delay and the security of the wireless network.

A. Backlogged Scenario

Since one message is split into two packets, the size of each packet is halved. When fixing the duration of the time slots, the requirement for the rate of the confidential message could be reduced from R_s to $R'_s = R_s/2$. The threshold for the rate of the eavesdropping link is also reduced from R_e to $R'_e = R_e/2$. Then, the rate threshold of codewords becomes $R'_t = R'_s + R'_e = (R_s + R_e)/2$.

Note that the mean delay is doubled since both of the two packets should be successful. By the similar derivations as

Theorem 1, we get the following corollary which gives the mean delay in the case of message split.

Corollary 1: The mean delay of the typical legitimate link in the backlogged scenario with message split is

$$\mathcal{D} = \frac{2}{p} \exp(\lambda_l \pi r_0^2 \theta_t'^\delta C(\delta) p (1-p)^{\delta-1}), \quad (24)$$

where $\theta_t' = 2^{R_t'} - 1$.

Comparing with the result given by (7), we observe that the mean delay is doubled and θ_t is replaced by θ_t' . However, since the effect of the two changes are in the opposite direction, whether the mean delay is increased or not is still uncertain, which depends on the parameters such as the transmit probability p , the intensity of legitimate transmitters λ_l , and so on.

In order to intercept the confidential message, both of the two packets from the same message should be successfully decoded at the eavesdropper. Therefore, by the similar derivations as that in Theorem 2, we get

Corollary 2: The secrecy outage probability of the typical link in the backlogged scenario with message split can be approximated by

$$\mathcal{P}_{so} \simeq \left(\frac{\exp\left(\frac{\lambda_e}{p \lambda_l \theta_e'^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{p \lambda_l \theta_e'^\delta C(\delta)}\right) + \exp(-p \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)) - 1} \right)^2, \quad (25)$$

where $\theta_e' = 2^{R_e'} - 1$.

The secrecy outage probability in the backlogged scenario with message split is closed-form. The result also reveals that $\mathcal{P}_{so} \rightarrow 0$ as $\lambda_e \rightarrow 0$, and $\mathcal{P}_{so} \rightarrow 1$ as $\lambda_e \rightarrow +\infty$. Though whether the message split decreases the secrecy outage probability is still not intuitive from Corollary 2, the numerical analysis could be conducted to evaluate the effect of message split.

B. Dynamic Scenario

The analysis of the dynamic scenario is different from that of the backlogged scenario when the message split is introduced in the transmission mechanism. The arrival process of the messages is still a Bernoulli process of arrival rate ξ . Since each message is split into two packets which are transmitted independently, at least two time slots are needed to successfully deliver one message. However, the queueing system is still a Geo/G/1 queue because the number of time slots between two adjacent arrivals is still a geometric random variable. When each message is divided into two packets, the service time of each message is the summation of the service time of the two packets. Since the service time of each packet is a geometric random variable, the total service time for each message is the summation of two geometric distributed random variables. The analysis of this queueing system is rather difficult because the service rate is not a well know distribution. Thus, we use the formula for the mean delay obtained from the M/M/1 queueing system to approximate the mean delay in the dynamic scenario with message split. With these discussions, we get the following corollary, which

gives the mean delay in the dynamic scenario with message split.

Corollary 3: The mean delay of the typical legitimate link in the dynamic scenario with message split is

$$\mathcal{D} \simeq -\frac{1}{\frac{p \xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)}{2 \mathcal{W}(-\xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta))} + \xi}, \quad (26)$$

where $\theta_t' = 2^{R_t'} - 1$.

Proof: By approximating the queueing system with the M/M/1 model, the mean delay can be approximated as

$$\mathcal{D} \simeq \frac{1}{\mu - \xi}, \quad (27)$$

where ξ is the arrival rate of the messages, and μ is the service rate. The mean delay in the dynamic scenario with message split could be obtained by the service rate of the Geo/G/1 queue.

Similar to the derivations in Theorem 3, the connection failure probability of a packet is

$$\mathcal{P}_{cf} = \min \left\{ 1 + \frac{\xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)}{\mathcal{W}(-\xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta))}, 1 - \xi \right\}, \quad (28)$$

where $\theta_t' = 2^{R_t'} - 1$. The service time for each packet is a geometric random variable with success probability $p(1 - \mathcal{P}_{cf})$, and the mean service time for each packet is $\frac{1}{p(1 - \mathcal{P}_{cf})}$. Thus, the mean service time for each message is $\frac{1}{p(1 - \mathcal{P}_{cf})}$, and the mean service rate for each message is $\frac{p(1 - \mathcal{P}_{cf})}{2}$. Plugging into the equation (27), we get the mean delay as

$$\mathcal{D} \simeq -\frac{1}{\frac{p \xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)}{2 \mathcal{W}(-\xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta))} + \xi}. \quad (29)$$

Therefore, we get the result in the corollary. \square

By the expansion of the Lambert- \mathcal{W} function given by the equation (17), we get the mean delay when $\lambda_l \pi r_0^2 \theta_t'^\delta C(\delta) \rightarrow 0$ as

$$\begin{aligned} \mathcal{D} &\simeq \frac{1}{\frac{p}{2(1 + \xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta))} - \xi} \\ &\simeq \frac{2}{p - 2\xi}. \end{aligned} \quad (30)$$

Furthermore, when $p = 1$ and $\xi \rightarrow 0$, the mean delay \mathcal{D} is exactly two time slots, which is the case where the transmission attempts of a packet is scheduled with probability one and is always successful when it is scheduled.

To eavesdrop the confidential message at an eavesdropper in the dynamic scenario with message split, both of the two packets from the same message should be successfully decoded at the eavesdropper. By the similar derivations as that in Theorem 4, we get

Corollary 4: The secrecy outage probability of the typical link in the dynamic scenario with message split can be approximated by

$$\mathcal{P}_{so} \simeq \left(\frac{\exp\left(\frac{\lambda_e}{q^* \lambda_l \theta_e'^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{q^* \lambda_l \theta_e'^\delta C(\delta)}\right) + \exp(-q^* \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)) - 1} \right)^2, \quad (31)$$

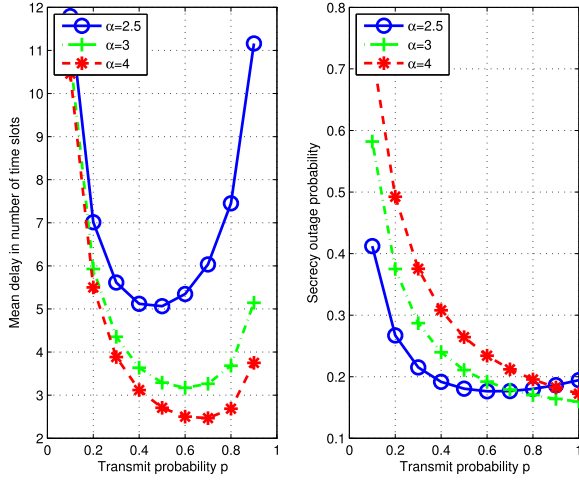


Fig. 5. The mean delay and the secrecy outage probability as functions of the transmit probability p in the backlogged scenario.

where q^* is given by

$$q^* = \min \left\{ -\frac{\mathcal{W}(-\xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta))}{\lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)}, 1 \right\}, \quad (32)$$

$\theta_t' = 2^{R_t} - 1$, and $\theta_e' = 2^{R_e} - 1$.

Specially, when $\lambda_l \pi r_0^2 \theta_t'^\delta C(\delta) \rightarrow 0$, using the expansion of the Lambert- \mathcal{W} function given by (17), we obtain

$$q^* = \min\{\xi, 1\}, \quad (33)$$

When the queue is stable, the arrival rate of messages must be smaller than one, i.e., $\xi < 1$. Therefore, we have

$$q^* = \xi. \quad (34)$$

Then, the secrecy outage probability given by Corollary 4 could be simplified as

$$\begin{aligned} P_{so} &\simeq \left(\frac{\exp\left(\frac{\lambda_e}{\xi \lambda_l \theta_e'^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{\xi \lambda_l \theta_e'^\delta C(\delta)}\right) + \exp\left(-\xi \lambda_l \pi r_0^2 \theta_t'^\delta C(\delta)\right) - 1} \right)^2 \\ &\simeq \left(1 - \exp\left(-\frac{\lambda_e}{\xi \lambda_l \theta_e'^\delta C(\delta)}\right) \right)^2. \end{aligned} \quad (35)$$

V. NUMERICAL EVALUATION

In this section, we evaluate the tradeoff between the mean delay and the secrecy outage probability through numerical analysis to gain insight. Without special explanation, the numerical parameters are set as follows in default. The intensities of the legitimate transmitters and the eavesdroppers are set as $\lambda_l = 0.05$ and $\lambda_e = 0.01$, respectively, and the desired link distance is $r_0 = 1$. The path loss exponent is $\alpha = 4$, the transmit probability is $p = 0.8$, and the packet arrival rate is $\xi = 0.1$. The rate threshold of codewords is $R_t = 3$ bits/Hz, and that of confidential messages is $R_e = 1$ bit/Hz.

Figure 5 shows the mean delay and the secrecy outage probability as functions of the transmit probability p in the backlogged scenario. As p increases, both the mean delay and the secrecy outage probability first decrease then increase. When p starts to increase, the mean delay decreases since

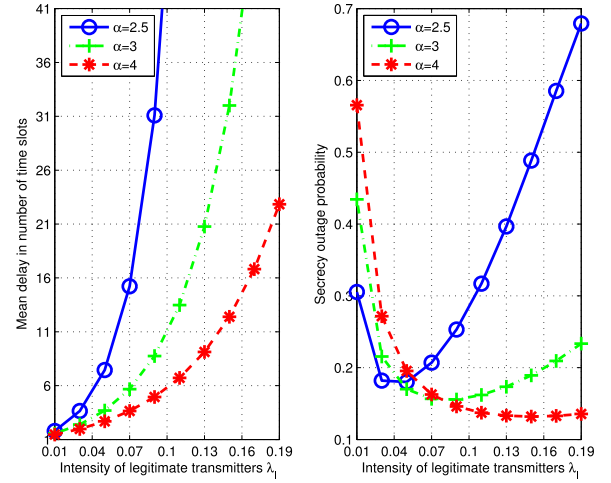


Fig. 6. The mean delay and the secrecy outage probability as functions of the intensity of legitimate transmitters λ_l in the backlogged scenario.

the successful delivery of a packet is limited by the transmit probability, while the secrecy outage probability decreases since the interference for the eavesdropping links increases. When p continues to grow, the mean delay increases since the interference increases, while the secrecy outage probability increases since the probability to eavesdrop the message is increased with large p . Figure 6 shows the mean delay and the secrecy outage probability as functions of λ_l in the backlogged scenario. When λ_l increases, the mean delay increases and the secrecy outage probability decreases since the interference in the network increases. However, when λ_l continues to grow, the secrecy outage probability increases since the distances of the eavesdropping links are decreased. Figure 7 plots the tradeoff between the mean delay and the secrecy outage probability when increasing λ_l in the backlogged scenario. Though the value of λ_l is not marked in Fig. 7, we can observe from Theorem 1 that λ_l is linear positive correlated to $\ln(D)$ which is the value of the horizontal ordinate. Note that when the path loss exponent α increases, the secrecy outage probability decreases for large λ_l and increases for small λ_l , indicating that the security performance is much better when the signal attenuates quickly (i.e., when α is large) for large λ_l , and it is reverse for small λ_l .

Figure 8 shows the mean delay and the secrecy outage probability as functions of the intensity of legitimate transmitters λ_l with different θ_t in the dynamic scenario. When varying θ_t , we keep the rate threshold of confidential messages R_s to be the same (i.e., $R_s = 1$ bits/Hz). Thus, the minimal confidential rate $R_s = 1$ is guaranteed. Figure 8 reveals that although the same confidential rate is guaranteed, the mean delay is larger and the secrecy outage probability is smaller in the high SIR regime than those in the low SIR regime.

Figure 9 and Figure 10 show the comparison of the mean delay and the secrecy outage probability for different scenarios with and without message split. The arrival rate is $\xi = 0.2$. Figure 9 reveals that in the backlogged scenario, the mean delay with message split is larger than that without message

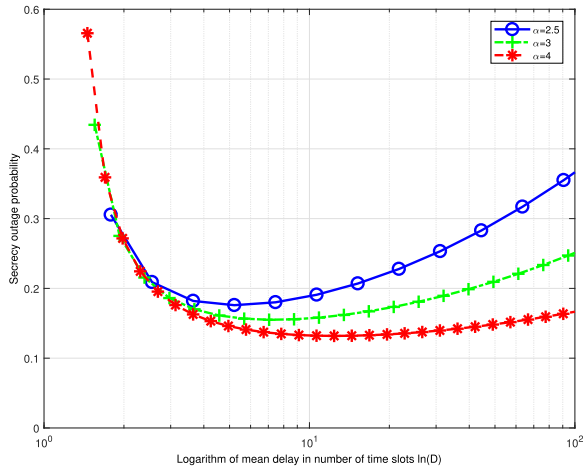


Fig. 7. Tradeoff between the mean delay and the secrecy outage probability when λ_l increases from 0.01 to 0.09 in the backlogged scenario.

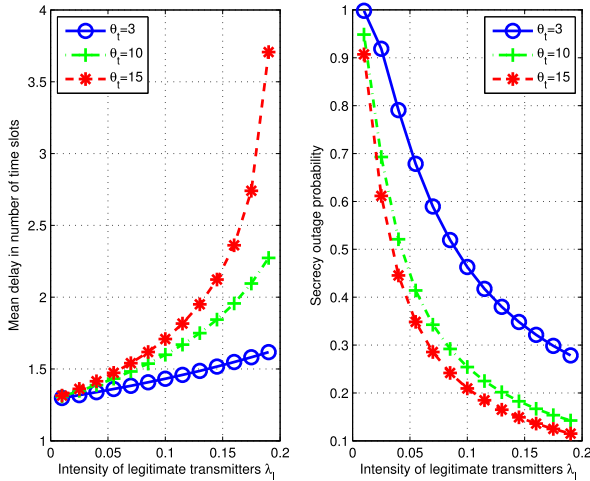


Fig. 8. The mean delay and the secrecy outage probability as functions of the intensity of legitimate transmitters λ_l in the dynamic scenario.

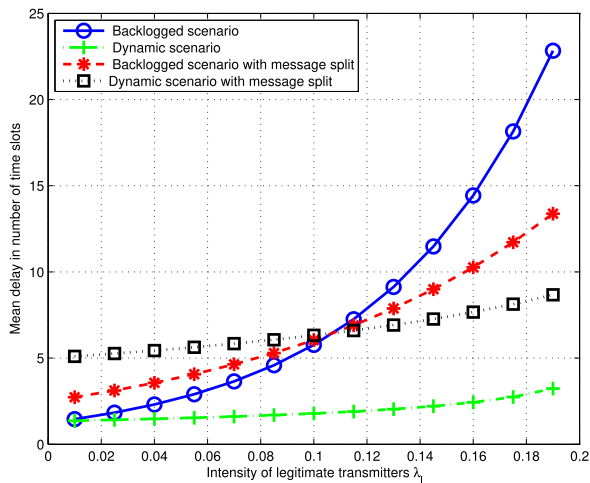


Fig. 9. Comparison of the mean delay in different scenarios with and without message split.

split when λ_l is small, while it is reverse for large λ_l , indicating that in the backlogged scenario, message split is beneficial for the delay performance only for large λ_l . Figure 9

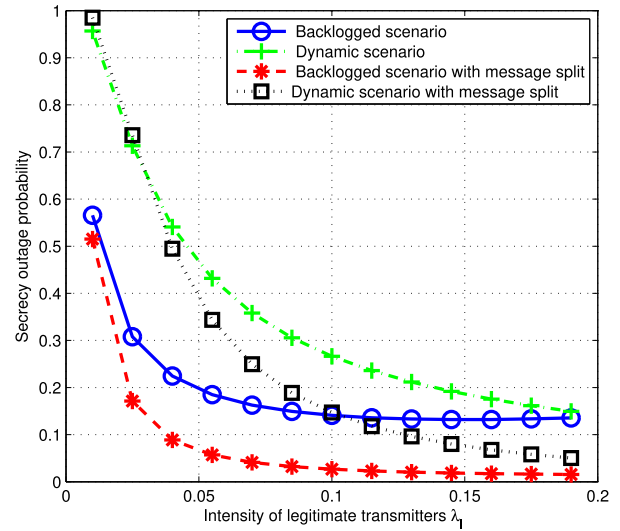


Fig. 10. Comparison of the secrecy outage probability in different scenarios with and without message split.

also reveals that in the dynamic scenario, the delay performance without message split is always better than that with message split. Figure 10 shows that in the backlogged scenario, introducing message split greatly decreases the secrecy outage probability and improves the security performance, while in the dynamic scenario, introducing message split is only beneficial when λ_l is large. Accordingly, in the actual application scenario such as the military communications, the message split scheme could be introduced to improve the security performance at the expense of increasing the delay when the density of the soldiers in the communications is not very small.

VI. CONCLUSION

In this work, we evaluate the tradeoff between the delay and the security performance in large wireless networks for both the backlogged scenario and the dynamic scenario. By combining the tools from stochastic geometry and queueing theory, we derive the close-formed results for the mean delay and the secrecy outage probability. We also analyzed the effect of a simple transmission mechanism which splits a message into two packets.

Our results reveal that the security performance of a large wireless network is better for larger path loss exponent when the density of legitimate nodes is large, and it is reverse when the density is small. We also observe that under the condition that a certain confidential rate is guaranteed, the delay performance is better in high SIR regime than that in low SIR regime. Moreover, by introducing the simple mechanism of message split, it is shown that the delay performance in the backlogged scenario is improved when the density of the legitimate transmitters is large. Meanwhile, introducing message split greatly improves the security performance in the backlogged scenario, while slightly improves the security performance in the dynamic scenario when the density of the legitimate transmitters is large.

APPENDIX A
PROOF OF THEOREM 2

Let $\Phi_k \subset \Phi_l$ be the set of transmitters that are active in time slot k , and let I_k be the interference at the typical legitimate receiver located at x_0 in time slot k . Then, the mathematical expression for I_k is

$$I_k = \sum_{y \in \Phi_l} h_y |y - x_0|^{-\alpha} \mathbf{1}(y \in \Phi_k). \quad (36)$$

With given Φ_l , the connection failure probability is

$$\begin{aligned} \mathcal{P}_{\text{cf}}^{\Phi_l} &= \mathbb{P}(h_{x_0} r_0^{-\alpha} < \theta_l I_k \mid \Phi_l) \\ &\stackrel{(a)}{=} 1 - \mathbb{E}[\exp(-\theta_l r_0^\alpha I_k) \mid \Phi_l] \\ &= 1 - \mathbb{E}\left[\exp\left(-\sum_{y \in \Phi_l} \theta_l r_0^\alpha h_y |y - x_0|^{-\alpha} \mathbf{1}(y \in \Phi_k)\right) \mid \Phi_l\right] \\ &= 1 - \prod_{y \in \Phi_l} \left(p \mathbb{E}\left[\exp(-\theta_l r_0^\alpha h_y |y - x_0|^{-\alpha}) \mid \Phi_l\right] + 1 - p\right) \\ &\stackrel{(b)}{=} 1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_l r_0^\alpha |y - x_0|^{-\alpha}} + 1 - p\right) \\ &\stackrel{(c)}{=} 1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_l r_0^\alpha |y|^{-\alpha}} + 1 - p\right), \end{aligned} \quad (37)$$

where (a) and (b) follow because the fading coefficients $\{h_y\}$ are i.i.d. exponential distributed random variables with unit mean, (c) holds due to the stationarity of the PPP.

With given Φ_l and Φ_e , the secrecy failure probability is

$$\begin{aligned} \mathcal{P}_{\text{sf}}^{\Phi_l, \Phi_e} &= 1 - \prod_{x_e \in \Phi_e} \mathbb{P}\{\text{SIR}_{x_e} < \theta_e \mid \Phi_l, \Phi_e\} \\ &= 1 - \prod_{x_e \in \Phi_e} \mathbb{P}\{h_e |x_e|^{-\alpha} < \theta_e I_k \mid \Phi_l, \Phi_e\} \\ &= 1 - \prod_{x_e \in \Phi_e} \left(1 - \mathbb{E}[\exp(-\theta_e I_k |x_e|^\alpha) \mid \Phi_l, \Phi_e]\right) \\ &= 1 - \prod_{x_e \in \Phi_e} \left(1 - \mathbb{E}\left[\exp(-\theta_e |x_e|^\alpha \sum_{y \in \Phi_l} h_y |y - x_e|^{-\alpha} \times \mathbf{1}(y \in \Phi_k)) \mid \Phi_l, \Phi_e\right]\right) \\ &= 1 - \prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \mathbb{E}[\exp(-\theta_e |x_e|^\alpha h_y |y - x_e|^{-\alpha} \times \mathbf{1}(y \in \Phi_k)) \mid \Phi_l, \Phi_e]\right) \\ &= 1 - \prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right). \end{aligned} \quad (38)$$

From equation (8), we get the secrecy outage probability of the typical link as

$$\begin{aligned} \mathcal{P}_{\text{so}} &= \mathbb{E}_{\Phi_l, \Phi_e} \left[\frac{\mathcal{P}_{\text{sf}}^{\Phi_l, \Phi_e}}{1 - \mathcal{P}_{\text{cf}}^{\Phi_l} (1 - \mathcal{P}_{\text{sf}}^{\Phi_l, \Phi_e})} \right] \\ &= \mathbb{E}_{\Phi_l, \Phi_e} \left[\left(1 - \prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right)\right) \left(1 - \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_l r_0^\alpha |y|^{-\alpha}} + 1 - p\right)\right)\right) \right] \end{aligned}$$

$$\times \prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right)^{-1}. \quad (39)$$

To derive the exact secrecy outage probability is difficult, and we propose to approximate the secrecy outage probability. Using the Jensen's inequality to approximate the secrecy outage probability, i.e., $\mathbb{E}_X(f(X)) \simeq f_X(\mathbb{E}[X])$ for a random variable X and a function $f(\cdot)$, we get

$$\begin{aligned} \mathcal{P}_{\text{so}} &\simeq \left(1 - \mathbb{E}_{\Phi_l, \Phi_e} \left[\prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right)\right]\right) \left(1 - \left(1 - \mathbb{E}_{\Phi_l} \left[\prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_l r_0^\alpha |y|^{-\alpha}} + 1 - p\right)\right]\right)\right) \\ &\mathbb{E}_{\Phi_l, \Phi_e} \left[\prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right)\right]^{-1}. \end{aligned} \quad (40)$$

Using the probability generating functional (PGFL) of the PPP, we have

$$\begin{aligned} \mathbb{E}_{\Phi_l} \left[\prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_l r_0^\alpha |y|^{-\alpha}} + 1 - p\right) \right] &= \exp\left(-\lambda_l \int_{\mathbb{R}^2} \left(1 - \left(\frac{p}{1 + \theta_l r_0^\alpha |y|^{-\alpha}} + 1 - p\right)\right) dy\right) \\ &= \exp(-p \lambda_l \pi r_0^2 \theta_l^\delta C(\delta)). \end{aligned} \quad (41)$$

Due to the stationarity of the PPP and the independence between Φ_l and Φ_e , we have

$$\begin{aligned} \mathbb{E}_{\Phi_l, \Phi_e} \left[\prod_{x_e \in \Phi_e} \left(1 - \prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right)\right] &= \mathbb{E}_{\Phi_e} \left[\prod_{x_e \in \Phi_e} \left(1 - \mathbb{E}_{\Phi_l} \left[\prod_{y \in \Phi_l} \left(\frac{p}{1 + \theta_e |x_e|^\alpha |y - x_e|^{-\alpha}} + 1 - p\right)\right]\right)\right] \\ &= \mathbb{E}_{\Phi_e} \left[\prod_{x_e \in \Phi_e} \left(1 - \exp(-p \lambda_l \pi |x_e|^2 \theta_e^\delta C(\delta))\right)\right] \\ &= \exp\left(-\lambda_e \int_{\mathbb{R}^2} \exp(-p \lambda_l \pi |x|^2 \theta_e^\delta C(\delta)) dx\right) \\ &= \exp\left(-\frac{\lambda_e}{p \lambda_l \theta_e^\delta C(\delta)}\right). \end{aligned} \quad (42)$$

Plugging into the equation (40), we have $\mathcal{P}_{\text{so}} \simeq$

$$\begin{aligned} &\frac{1 - \exp\left(-\frac{\lambda_e}{p \lambda_l \theta_e^\delta C(\delta)}\right)}{1 - \exp\left(-\frac{\lambda_e}{p \lambda_l \theta_e^\delta C(\delta)}\right) + \exp\left(-p \lambda_l \pi r_0^2 \theta_l^\delta C(\delta) - \frac{\lambda_e}{p \lambda_l \theta_e^\delta C(\delta)}\right)} \\ &= \frac{\exp\left(\frac{\lambda_e}{p \lambda_l \theta_e^\delta C(\delta)}\right) - 1}{\exp\left(\frac{\lambda_e}{p \lambda_l \theta_e^\delta C(\delta)}\right) + \exp\left(-p \lambda_l \pi r_0^2 \theta_l^\delta C(\delta)\right) - 1}. \end{aligned} \quad (43)$$

Therefore, we get the results in the theorem.

REFERENCES

- [1] Y. Zhong, T. Han, Q. Li, and X. Ge, "Delay and physical layer security tradeoff in large wireless networks," to be published.
- [2] X. Ge, S. Tu, G. Mao, and C. X. Wang, "5G ultra-dense cellular networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

- [3] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.
- [4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [5] X. Ge, Z. Li, and S. Li, "5G software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 87–93, Jul. 2017.
- [6] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
- [7] Y. Zhong, T. Q. S. Quek, and X. Ge, "Heterogeneous cellular networks with spatio-temporal traffic: Delay analysis and scheduling," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1373–1386, Jun. 2017.
- [8] Y. Zhong, M. Haenggi, F.-C. Zheng, W. Zhang, T. Q. S. Quek, and W. Nie, "Toward a tractable delay analysis in ultra-dense networks," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 103–109, Dec. 2017.
- [9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
- [10] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
- [11] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2466–2470.
- [12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [13] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
- [14] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
- [15] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
- [16] 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, Jul. 2016.
- [17] Y. Wu, J.-B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3614–3628, Aug. 2017.
- [18] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
- [19] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 539–543.
- [20] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "The effect of eavesdroppers on network connectivity: A secrecy graph approach," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 712–724, Sep. 2011.
- [21] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in *Proc. Int. Symp. Inf. Theory Appl.*, Oct. 2010, pp. 349–354.
- [22] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.
- [23] A. Sarkar and M. Haenggi, "Secrecy coverage," in *Proc. Conf. Rec. 44th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2010, pp. 42–46.
- [24] O. O. Koyluoglu, C. E. Koksall, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.
- [25] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs under passive and active attacks," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6692–6702, Oct. 2011.
- [26] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.
- [27] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
- [28] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "Stochastic analysis of spatial and opportunistic Aloha," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1105–1119, Sep. 2009.
- [29] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.
- [30] J. Wen, M. Sheng, X. Wang, J. Li, and H. Sun, "On the capacity of downlink multi-hop heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4092–4103, Aug. 2014.
- [31] M. Sheng, J. Wen, J. Li, B. Liang, and X. Wang, "Performance analysis of heterogeneous cellular networks with HARQ under correlated interference," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 8377–8389, Dec. 2017.
- [32] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
- [33] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1928–1939, Sep. 2016.
- [34] X. Zhu, B. Yang, C. Chen, L. Xue, X. Guan, and F. Wu, "Cross-layer scheduling for OFDMA-based cognitive radio systems with delay and security constraints," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5919–5934, Dec. 2015.
- [35] B. Blaszczyszyn, M. Jovanovic, and M. K. Karray, "Performance laws of large heterogeneous cellular networks," in *Proc. IEEE 13th Inter. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw. (WiOpt)*, May 2015, pp. 597–604.
- [36] R. R. Rao and A. Ephremides, "On the stability of interacting queues in a multiple-access system," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 5, pp. 918–930, Sep. 1988.
- [37] W. Luo and A. Ephremides, "Stability of N interacting queues in random-access systems," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1579–1587, Jul. 1999.
- [38] A. Ephremides and R.-Z. Zhu, "Delay analysis of interacting queues with an approximate model," *IEEE Trans. Commun.*, vol. COM-35, no. 2, pp. 194–201, Jan. 1987.
- [39] Y. Zhong, M. Haenggi, T. Q. S. Quek, and W. Zhang, "On the stability of static poisson networks under random access," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2985–2998, Jul. 2016.
- [40] W. Feng, Y. Wang, D. Lin, N. Ge, J. Lu, and S. Li, "When mmWave communications meet network densification: A scalable interference coordination perspective," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1459–1471, Jul. 2017.
- [41] M. Haenggi, "The local delay in Poisson networks," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1788–1802, Mar. 2013.
- [42] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.
- [43] Y. Zhong, W. Zhang, and M. Haenggi, "Managing interference correlation through random medium access," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 928–941, Feb. 2014.
- [44] I. Atencia and P. Moreno, "A discrete-time Geo/G/1 retrial queue with general retrial times," *Queueing Syst.*, vol. 48, nos. 1–2, pp. 5–21, 2004.
- [45] G. Falin, "A survey of retrial queues," *Queueing Syst.*, vol. 7, no. 2, pp. 127–167, Jun. 1990.



Yi Zhong (S'12–M'15) received the B.S. and Ph.D. degrees in electronic engineering from the University of Science and Technology of China in 2010 and 2015, respectively. In 2012, he was a Visiting Student with the Prof. M. Haenggi's Group, University of Notre Dame. In 2013, he was a Research Intern with Qualcomm Incorporated, Corporate Research and Development, Beijing. From 2015 to 2016, he was a Post-Doctoral Research Fellow with the Wireless Networks and Decision Systems Group led by Prof. T. Q. S. Quek, Singapore University of Technology and Design. He is currently an Assistant Professor with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China. His main research interests include heterogeneous and femtocell-overlaid cellular networks, wireless ad hoc networks, stochastic geometry, and point process theory.



Xiaohu Ge (M'09–SM'11) received the Ph.D. degree in communication and information engineering from the Huazhong University of Science and Technology (HUST), China, in 2003. He has been with HUST since 2005. Prior to that, he was a Researcher with Ajou University, South Korea, and with the Politecnico di Torino, Italy, from 2004 to 2005. He is currently a Full Professor with the School of Electronic Information and Communications, HUST. He is also an Adjunct Professor with the Faculty of Engineering and Information

Technology, University of Technology Sydney, Australia. He is the Director of the China International Joint Research Center of Green Communications and Networking. He has authored or co-authored about 180 papers in refereed journals and conference proceedings. He has been granted about 15 patents in China. His research interests are mobile communications, traffic modeling in wireless networks, green communications, and interference modeling in wireless communications. He was a recipient of the Best Paper Awards from the IEEE GLOBECOM 2010. He has been actively involved in organizing over 10 international conferences since 2005. He served as the General Chair of the 2015 IEEE International Conference on Green Computing and Communications. He serves as an Editor for the IEEE WIRELESS COMMUNICATIONS and the IEEE TRANSACTION ON GREEN COMMUNICATIONS AND NETWORKING.



Tao Han (M'13) received the bachelor's degree in information engineering, the master's degree in communication and information system, and the Ph.D. degree in information and communication engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 1990, 1993, and 2001, respectively. From 2010 to 2011, he was a Visiting Scholar with the University of Florida, Gainesville, FL, USA, as a Courtesy Associate Professor. He was a Visiting Professor with the University of Technology Sydney, Ultimo, NSW,

Australia, in 2016. He is currently an Associate Professor with the School of Electronic Information and Communications, HUST. He is also a Vice Chair of the China International Joint Research Center of Green Communications and Networking. His research interests include wireless communications, multimedia communications, and computer networks. He is leading several projects funded by the National Natural Science Foundation of China, the Ministry of Science and Technology of China, and industries. He is currently serving as an Area Editor for the *EAI Endorsed Transactions on Cognitive Communications*. He was a recipient of the IET Networks Premium Awards in 2017 and the Best Paper Awards from the IEEE CIC ICC 2017, the IEEE ISCT 2016, and the IEEE GLOBECOM 2010.



Qiang Li (M'16) received the B.Eng. degree from the University of Electronic Science and Technology of China, China, in 2007, and the Ph.D. degree from Nanyang Technological University (NTU), Singapore, in 2011. From 2011 to 2013, he was a Research Fellow with NTU. Since 2013, he has been an Associate Professor with the Huazhong University of Science and Technology, China. His research interests include next generation mobile communications, software-defined networking, full-duplex techniques, and wireless cooperative communications.



Jing Zhang (M'13) received the M.S. and Ph.D. degrees in electronics and information engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2002 and 2010, respectively. He is currently an Associate Professor with HUST. He has done research in the areas of multiple input multiple output, CoMP, beamforming, and next-generation mobile communications. His current research interests include HetNet in 5G, green communications, energy harvesting, Internet of Things, optimization, and performance analysis

in networks. He was a recipient of the Best Paper Award at the IEEE Globecom Communication Workshop in 2014 and the International Wireless Communications and Mobile Computing Conference in 2015.