Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 760175, 6 pages
http://dx.doi.org/10.1155/2014/760175

Research Article

Secure Wireless Communications via Cooperative Transmitting

Toni Draganov Stojanovski[1] and Ninoslav Marina[1,2]

[1] *University for Information Science and Technology "St. Paul the Apostle", 6000 Ohrid, Macedonia*
[2] *Ecole Polytechnique Federale de Lausanne, 1015 Lausanne, Switzerland*

Correspondence should be addressed to Toni Draganov Stojanovski; toni_stojanovski@ieee.org

Received 31 August 2013; Accepted 6 January 2014; Published 23 February 2014

Academic Editors: R. Bruno and Z. Cai

Information-theoretic secrecy is combined with cryptographic secrecy to create a secret-key exchange protocol for wireless networks. A network of transmitters, which already have cryptographically secured channels between them, cooperate to exchange a secret key with a new receiver at a random location, in the presence of passive eavesdroppers at unknown locations. Two spatial point processes, homogeneous Poisson process and independent uniformly distributed points, are used for the spatial distributions of transmitters and eavesdroppers. We analyse the impact of the number of cooperating transmitters and the number of eavesdroppers on the area fraction where secure communication is possible. Upper bounds on the probability of existence of positive secrecy between the cooperating transmitters and the receiver are derived. The closeness of the upper bounds to the real value is then estimated by means of numerical simulations. Simulations also indicate that a deterministic spatial distribution for the transmitters, for example, hexagonal and square lattices, increases the probability of existence of positive secrecy capacity compared to the random spatial distributions. For the same number of friendly nodes, cooperative transmitting provides a dramatically larger secrecy region than cooperative jamming and cooperative relaying.

1. Introduction

Information-theoretic secrecy has attracted a significant interest in recent years due to its possible applications in wireless communications and the growing significance of wireless networks. Wyner [1] first introduced the concept of wiretap channel in 1975. For discrete memoryless channels, he has determined that a message can be transmitted reliably from a transmitter to a receiver without revealing any information on the message to the eavesdropper provided that the transmitter operates at rates smaller than the secrecy capacity. If the main channel and the wiretap channel are additive white Gaussian noise channels, then the secrecy capacity is equal to the difference of the capacities of the two channels as shown by Leung-Yan-Cheong and Hellman in [2]. Csiszár and Körner [3] studied the case of a broadcast channel with confidential messages, in which the sender transmits common information to both the legitimate receiver and the wiretapper in addition to the confidential information to the legitimate receiver. They established the secrecy capacity region for this channel in which the message intended for the legitimate receiver is kept private.

Secrecy capacity can be improved using cooperation with friendly nodes [4]. In the *cooperative jamming* [5], friendly nodes, which are close to the eavesdropper, jam the eavesdropper to help increase the achievable secrecy rates for the transmitter by decreasing the signal-to-noise (SNR) ratio at the eavesdropper. In the *cooperative relaying* [6, 7], friendly nodes which are closer to the receiver than to the eavesdropper are used as relays. The relays increase SNR more at the receiver than at the eavesdroppers.

Information theory achieves perfect (unconditional) secrecy as opposed to the computational secrecy provided by cryptographic algorithms. Here we examine the possibility for mutual applications of cryptographic secrecy and information-theoretic secrecy. A set of transmitters have already cryptographically secured the communication channels between them. When a transmitter wants to communicate securely with a new receiver (e.g., a mobile station), a presecret key message is created by the transmitter and

broken into several data blocks, and a separate block is encrypted and sent to each of the other transmitters. Then each transmitter sends its data block to the receiver. The transmitters ensure that all the data blocks are received correctly at the receiving node, which is required for the computation of the secret key at the receiver. The secret key is securely and cooperatively transmitted to the receiver (without being divulged to the eavesdroppers) using information-theoretic secrecy if the secrecy capacity is positive for the communication channel between at least one transmitter and the receiver. As the number of transmitters grows, the eavesdroppers are facing a more difficult task of being able to intercept a larger number of transmitters. Once the secret key is exchanged, the legitimate parties can start communicating at the maximum data rate since their communication channel is cryptographically protected, achieving computational secrecy [8]. Our model and analysis are applicable to large scale cellular networks; the mobile carrier operates a high-speed backbone networks and the core-network infrastructures connecting individual base stations. Base stations rely on the core-network infrastructures to establish cryptographically secure channels between them. Transmitters correspond to the base stations, and the randomly located mobile users are modeled via the receivers. Large scale cellular networks are also analysed in [9, 10], where it is assumed that neighbouring base stations exchange information on the locations of the eavesdroppers, and therefore the locations of the eavesdroppers are known to a base station if they are in a neighbouring cell.

Our results are presented using the following organisation of the paper. In Section 2, we present the system model. In Section 3, we address the main research questions of this paper: (i) evaluation of the impact of the spatial distribution of transmitters and eavesdroppers on the secrecy region fraction and derivation of upper bounds for this fraction and (ii) comparison with cooperative relaying and cooperative jamming. Section 4 concludes the paper.

2. Network Model

We consider two-dimensional wireless networks with the following communication nodes: a network of L_T cooperating transmitters, a single receiver, and a network of L_E passive eavesdroppers. The passive eavesdroppers do not transmit any signal and try to intercept the information that is transmitted between the pairs of legitimate nodes, hence reducing the secrecy capability of the network. Their locations are unknown to the transmitters. Each transmitter is equipped with only a single omnidirectional antenna.

In the sequel, we use the following notation.

$L(A)$ is the area of a region $A \in R^2$;

L_T is a random variable which denotes the number of transmitters in a region A;

L_E is a random variable which denotes the number of eavesdroppers in a region A;

$b \parallel c$ is a concatenation of two data blocks b and c;

V, V_e are the additive noise at receiver and eavesdropper, which are independent zero mean Gaussian random variables with variance σ^2;

$C_{t,r}$ is the capacity of the communication channel between transmitter t and receiver r;

$C_{s:t,r}$ is the secrecy capacity between transmitter t and receiver r;

C_s is the secrecy capacity between a set of cooperating transmitters and a receiver;

$d_{j,i}$ is the distance between nodes i and j.

We use the additive white Gaussian noise model. Then, the received signal at the receiver r from the transmitter t is

$$Y = d_{t,r}^{-\beta/2} X + V, \tag{1}$$

where X is the transmitted signal from the transmitter t and β is the path-loss coefficient [11]. The received signal at the eavesdropper e from the transmitter t equals

$$Z_e = d_{t,e}^{-\beta/2} X + V_e. \tag{2}$$

The point to point capacities between transmitter t and receiver r, and between transmitter t and eavesdropper e are given by [2]

$$C_{t,r} = \frac{1}{2}\log_2\left(1 + \frac{P_t d_{t,r}^{-\beta}}{\sigma^2}\right), \qquad C_{t,e} = \frac{1}{2}\log_2\left(1 + \frac{P_t d_{t,e}^{-\beta}}{\sigma^2}\right), \tag{3}$$

where P_t is the transmitter's power. If the point to point capacity between the two communicating nodes $C_{t,r}$ is larger than the capacity of the channel between the transmitter and the eavesdropper $C_{t,e}$, then $C_{s:t,r} = C_{t,r} - C_{t,e} > 0$. Otherwise, $C_{s:t,r} = 0$ [2]:

$$C_{s:t,r} = \max\left\{C_{t,r} - C_{t,e}, 0\right\}. \tag{4}$$

From (3), it follows that $C_{s:t,r} > 0$ if the receiver r is closer to the transmitter than the eavesdropper; that is, $d_{t,r} < d_{t,e}$. The disk $D_s \subset R^2$ with center at the transmitter and radius equal to the distance between the transmitter and the nearest eavesdropper is called *secrecy disk* of the transmitter. If a receiver is inside the secrecy disk, then the secrecy capacity between the transmitter and the receiver is positive.

Receivers which are outside the secrecy disk for a given transmitter cannot communicate securely with that transmitter. In the next section, we explain a type of cooperation for a set of friendly transmitters that combines their secrecy disks and thus allows them to communicate secretly with receivers positioned in a larger region.

3. Cooperative Transmitting

The set of transmitters have already established a cryptographic secret key, and they can cryptographically protect their mutual communication channels. Let us assume that transmitter t_i and a new communicating node/receiver r

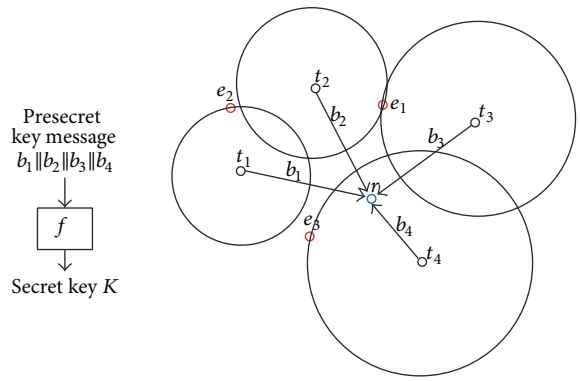

FIGURE 1: Sample network with four transmitters, one new receiver, and three eavesdroppers.

want to communicate. t_i generates a presecret key message B with arbitrary length, which it then divides into L_T blocks $b_1, b_2, \ldots, b_{L_T}$. Each block is sent to a different transmitter via a cryptographically secured channel. Then each transmitter t_i sends its block b_i to the receiver. The intended receiver correctly receives all blocks $b_1, b_2, \ldots, b_{L_T}$ and restores the presecret key message $B = b_1 \| b_2 \| \cdots \| b_{L_T}$. Both t_i and r use a cryptographic hash function H to calculate the mutual secret key $K = H(B)$, which is then used to cryptographically protect their mutual communication. The eavesdroppers have to be able to intercept the transmission from all L_T transmitters. If at least one data block out of L_T data blocks is not intercepted, then the secret key K cannot be computed at the eavesdropper. We call this strategy for cooperation—*cooperative transmitting*. Using cooperative transmitting, a transmitter can exchange a secret key with a receiver if the receiver is inside any of the secrecy disks for all L_T transmitters. The impact of cooperative transmitting is quantitatively measured through the fraction $F_s(A)$ of a region A covered by the union of secrecy disks. Fraction $F_s(A)$ is equal to the probability of securely exchanging a secretkey with a receiver that is randomly positioned inside the region A:

$$F_s(A) \equiv \mathbf{P}\{C_s > 0\}. \tag{5}$$

The coverage problem by secrecy disks was studied by Sarkar and Haenggi [12, 13]. They studied the covered volume fraction and the asymptotic conditions for complete coverage in one and two dimensions when $L(A) \to \infty$.

Figure 1 illustrates the concept of cooperative transmitting on a sample network. Receiver r is inside the secrecy disk of transmitter t_4, and therefore block b_4 cannot be intercepted by any of the eavesdroppers.

In the remainder of this paper, we analyse the dependence of $\mathbf{P}\{C_s > 0\}$ on the spatial distributions of transmitters and eavesdroppers. We analyse both random and deterministic models for the spatial distribution of transmitters and eavesdroppers. Two simple models for random spatial processes for the transmitters and the eavesdroppers will be used. The first model is homogeneous Poisson process on the plane characterised by the mean number of points λ in a unit area, also called *rate* or *density* of the Poisson Process. The number of points l inside a region A follows the Poisson probability distribution law with parameter $\lambda L(A)$:

$$P_L(l) = \frac{(\lambda L(A))^l}{l!} e^{-\lambda L(A)}. \tag{6}$$

In the second model, a fixed number of points are independently and uniformly distributed (IUD) in a certain region of the plane, characterised by a single parameter, the fixed number of points. These two models are widely used in the literature on information-theoretic secrecy [12–15], the reason being twofold. First, they provide a good first-order approximation for the spatial distribution of communication nodes in real networks. Recently [16, 17], it was shown that the two-dimensional homogeneous Poisson process-based model for the base stations' locations accurately estimates the behaviour of actual networks. The homogeneous Poisson process gives pessimistic lower bounds on coverage and throughput, while the deterministic grid model for the base stations' locations is optimistic. However, the two models provide an equally accurate prediction for the performances of an actual network of base stations [16]. Second, simplicity of the homogeneous Poisson process and the IUD process allows for an analytical analysis of information security-related metrics, for example, fraction $F_s(A)$. For the spatial distribution of the transmitters, we will also investigate two deterministic models: hexagonal lattice and square lattice.

3.1. IUD Transmitters and IUD Eavesdroppers. In the first case, the position of the transmitters in a region $A \in R^2$ obeys a IUD process with parameter n_T. A fixed number of eavesdroppers n_E are positioned according to an IUD process in the same region A. If $n_T = 1$, then $C_s > 0$ if the receiver is inside the secrecy disk of the transmitter, that is, the receiver is closer to the transmitter than any of the n_E eavesdroppers:

$$\mathbf{P}\{C_s > 0\} = \frac{1}{1 + n_E}. \tag{7}$$

For $n_T > 1$, we establish an upper bound for $\mathbf{P}\{C_s > 0\}$ as follows. For $n_T = 2$, the secrecy region of the two transmitters is a union of their secrecy disks:

$$\begin{aligned} \mathbf{P}\{C_s > 0\} &= 1 - \mathbf{P}\{C_s < 0\} \\ &\le 1 - \mathbf{P}\{C_{s:1,r} < 0\}\,\mathbf{P}\{C_{s:2,r} < 0\} \\ &= 1 - \left(\frac{n_E}{1 + n_E}\right)^2, \end{aligned} \tag{8}$$

where the overlapping area of the two secrecy disks is neglected in the upper bound. One can generalise (8) for $n_T > 1$, thus obtaining

$$\mathbf{P}\{C_s > 0\} \le 1 - \left(\frac{n_E}{1 + n_E}\right)^{n_T}. \tag{9}$$

Next we consider the case when both n_T and n_E grow infinitely, while their ratio remains constant $k = (n_T/n_E)$.

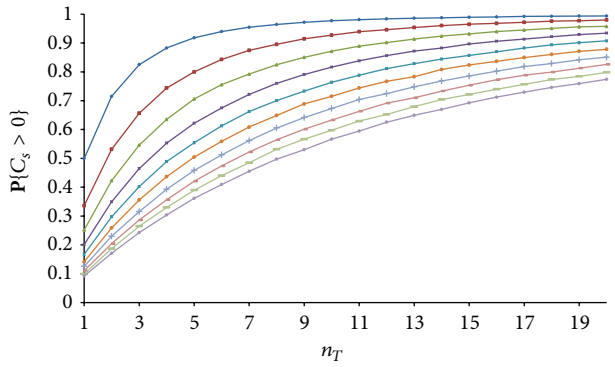

Figure 2: Dependence of $\mathbf{P}\{C_s > 0\}$ on the number of transmitters n_T with n_E as the curves' parameter. The lowest curve corresponds to $n_E = 10$, and the highest curve is for $n_E = 1$.

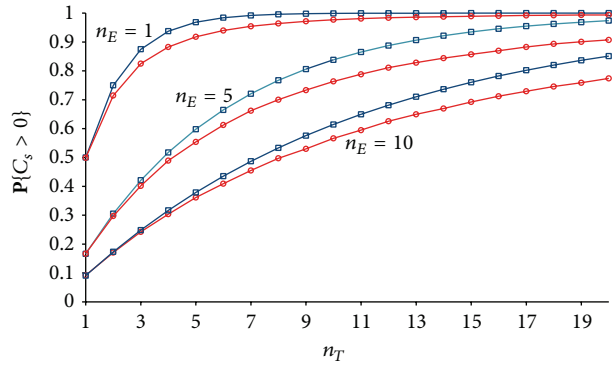

Figure 3: Closeness between the real value for $\mathbf{P}\{C_s > 0\}$ (circles) and the upper bound (squares) given by (9).

This is a good first-order approximation when the area of region A grows infinitely and the densities of transmitters and eavesdroppers remain constant. Then

$$\lim_{n_E \to \infty} \mathbf{P}\{C_s > 0\} \leq \lim_{n_E \to \infty} 1 - \left(\frac{n_E}{1 + n_E}\right)^{kn_E} = 1 - e^{-k}. \quad (10)$$

In order to evaluate the accuracy of the upper bounds (9) and (10), we have numerically estimated the value for $\mathbf{P}\{C_s > 0\}$ for real networks. Figure 2 depicts the dependence of $\mathbf{P}\{C_s > 0\}$ on n_T and n_E as obtained from the numerical simulations. Each point on the curves is averaged over 100,000 simulations of real networks.

Figure 3 shows the closeness between the upper bound given by (9) and the real values for $\mathbf{P}\{C_s > 0\}$, which are estimated through numerical simulations. Relative gap between the upper bound and the real values grows for larger n_T due to the increasing number of overlapping secrecy disks (see (8)).

Figure 4 shows the closeness between the upper bounds (9) and (10) and the numerically estimated values for $\mathbf{P}\{C_s > 0\}$. The relative gap between the upper bounds and the real values gets smaller for smaller k (larger n_E) since the secrecy disks as well as their overlaps become smaller in size. Consequently, the neglected terms in (8) become less significant.

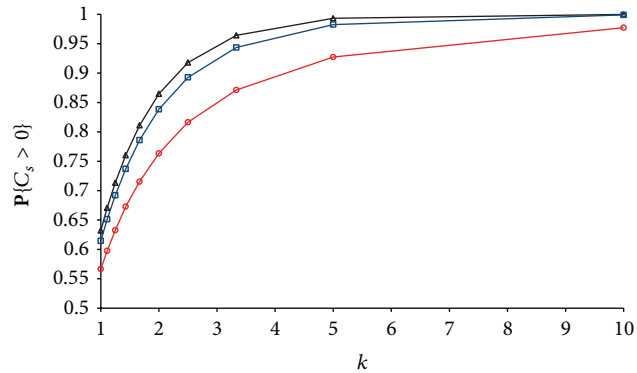

Figure 4: Closeness between the real value for $\mathbf{P}\{C_s > 0\}$ (circles) and the upper bounds given by (9) (squares) and (10) (triangles). $n_T = 10$ and $n_E = 1, 2, \ldots, 10$.

3.2. Poisson Transmitters and IUD Eavesdroppers. Next we consider the case where the transmitters are positioned according to a Poisson spatial process with rate λ_T. Without loss of generality of the results, we assume that $L(A) = 1$ and thus the average number of transmitters in the region A is $\lambda L(A) = \lambda$. The eavesdroppers' positions obey an IUD process and the number of eavesdroppers in the region A is n_E.

If the number of transmitters L_T is 1, then (7) holds. For $L_T > 1$, the upper bound given by (9) is valid. Then an upper bound for $\mathbf{P}\{C_s > 0\}$ can be derived as an average value of functions (7) and (9) for the random variable L_T:

$$\begin{aligned}\mathbf{P}\{C_s > 0\} &= E\left[\mathbf{P}\{C_s > 0 \mid L_T\}\right] \\ &\leq \frac{1}{1 + n_E}\lambda_T e^{-\lambda_T} \\ &\quad + \sum_{l_T=2}^{\infty}\left(1 - \left(\frac{n_E}{1 + n_E}\right)^{l_T}\right)\frac{\lambda_T^{l_T}}{l_T!}e^{-\lambda_T} \\ &= 1 - e^{-\lambda_T/(1+n_E)}.\end{aligned} \quad (11)$$

Figure 5 shows the closeness between the upper bound (11) and the numerically calculated values for $\mathbf{P}\{C_s > 0\}$. Similar to Figure 3, accuracy of the upper bound decreases for larger λ_T as a consequence of the increasing number of intersecting secrecy disks. Numerical simulation of a Poisson spatial process was done according to [18]. In order to generate a Poisson process with rate λ in a region A, we first randomly select a value l for a Poisson variable with mean $\lambda L(A)$, and then we randomly position l IUD points in A. Observed dependence of $\mathbf{P}\{C_s > 0\}$ on λ_T and n_E was similar to the one depicted in Figure 2.

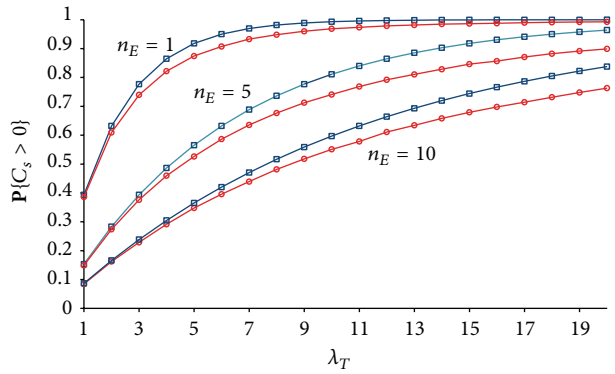

Figure 5: Closeness between the real value for $\mathbf{P}\{C_s > 0\}$ and the upper bound given by (11).

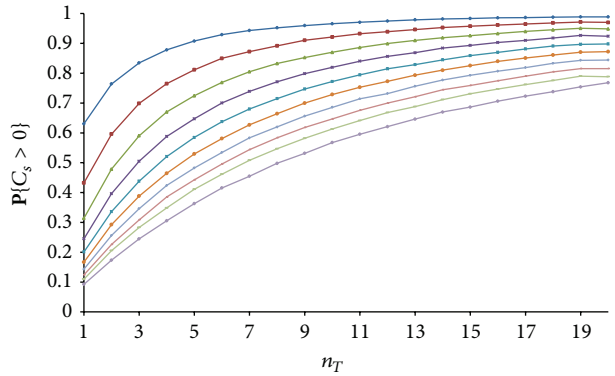

Figure 6: Dependence of $\mathbf{P}\{C_s > 0\}$ on the number of transmitters n_T with λ_E as the curves' parameter. The lowest curve corresponds to $\lambda_E = 10$, and the highest curve is for $\lambda_E = 1$.

3.3. IUD Transmitters and Poisson Eavesdroppers. A fixed number of transmitters n_T are positioned at IUD points in a region $A \in R^2$. The positions of the eavesdroppers follow a Poisson spatial process with average rate λ_E. For the sake of simplicity we again assume that $L(A) = 1$. Then the number of eavesdroppers in A is a Poisson random variable L_E with average value λ_E. Its probability distribution function is given by (6) where $\lambda = \lambda_E$. If there is only one transmitter randomly positioned in A, that is, $n_T = 1$, then the secrecy region fraction is given by

$$\mathbf{P}\{C_s > 0\} = E\left[\frac{1}{1 + L_E}\right] = \frac{1}{\lambda_E}\left(1 - e^{-\lambda_E}\right). \quad (12)$$

For $n_T > 1$, we ran numerical simulations, and the results are given in Figure 6. Note the similarity to Figure 2.

For the sake of completeness, we have also numerically analysed the case when a homogeneous Poisson process in a region $A \in R^2$ is assumed for both the transmitters and the eavesdroppers. Again we have obtained very similar results to the previously analysed three combinations of IUD and Poisson spatial processes for transmitters and eavesdroppers. Following slight differences were observed. IUD spatial process for the transmitters gives slightly higher values for $\mathbf{P}\{C_s > 0\}$ than the Poisson spatial processes. On the contrary, the Poisson spatial process for the eavesdroppers gives slightly higher values for $\mathbf{P}\{C_s > 0\}$ than the IUD spatial processes.

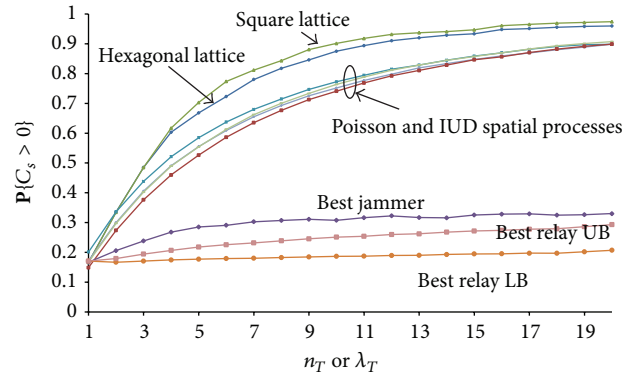

Figure 7: Comparison of stochastic and deterministic positioning of transmitters. Top two curves are for hexagonal and square lattice (IUD eavesdroppers with $n_E = 5$), while middle four curves are for Poisson and IUD spatial processes for the transmitters' and eavesdroppers' positions (with $\lambda_E = 5$ or $n_E = 5$). Bottom three curves are for cooperative jamming and cooperative relaying strategies for cooperation between transmitters.

3.4. Transmitters in Deterministic Lattice and UID Eavesdroppers. Next we analysed the case when the transmitters are positioned on a deterministic lattice, and the eavesdroppers obey a UID process. By means of numerical simulations we examined a square lattice and a hexagonal lattice. We observed similar shapes to the curves shown in Figures 2 and 6 for stochastic spatial processes for the transmitters. $\mathbf{P}\{C_s > 0\}$ is higher for a deterministic lattice compared to stochastic spatial processes for the transmitters (see Figure 7) due to the lower variations in the overlap between the secrecy disks of individual transmitters. For a stochastic spatial process, there are areas which can be covered by multiple overlapping secrecy disks of nearby transmitters. At the same time in the regions with sparse transmitters, it is more probable to find subregions not covered by any secrecy disk.

3.5. Comparison with Cooperative Jamming and Cooperative Relaying. In this section, we compare cooperative transmitting with two other strategies for cooperation in wireless networks. Cooperative relaying and cooperative jamming increase the secrecy capacity by means of widening the gap between the SNR at the legitimate receiver and the SNR at the eavesdroppers. In the single hop cooperation with the best relay [19, 20], only the strongest relay is selected from the set of UID randomly positioned relays, which is the relay node which most improves the secrecy capacity. In the "single hop cooperation with the best jammer" [19, 20], a single node from the set of friendly nodes is selected to act as a jammer. Cooperative jamming aims to reduce the SNR at the legitimate receiver, but at the same time it reduces the SNR even more at the eavesdroppers. On the contrary, the best relay increases the secrecy capacity by increasing SNR

at the legitimate receiver more than it increases SNR at the eavesdroppers.

We use the value for $\mathbf{P}\{C_s > 0\}$ as a quantitative measure of the positive impact of the different strategies for cooperation. Figure 7 shows that cooperative transmitting offers dramatic improvement in the secrecy region's size over cooperative jamming and cooperative relaying.

4. Conclusion

In this work, we propose to combine information-theoretic secrecy with cryptographic secrecy to increase the secrecy region and provide a novel solution to the key-exchange problem. Cooperative transmitting can significantly improve information-theoretic secrecy in wireless networks. The type of cooperation is quite important for the resulting secrecy region. For the same number of friendly nodes, cooperative transmitting provides a larger coverage area than cooperative jamming and cooperative relaying.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM '12)*, A. G. Greenberg and K. Sohraby, Eds., pp. 1152–1160, IEEE, 2012.

[5] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Proceedings of the Information Theory and Applications Workshop (ITA '07)*, pp. 404–413, February 2007.

[6] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[7] N. Marina, R. Bose, and A. Hjørungnes, "Increasing the secrecy capacity by cooperation in wireless networks," in *Proceedings of the IEEE 20th Personal, Indoor and Mobile Radio Communications Symposium (PIMRC '09)*, pp. 1978–1982, September 2009.

[8] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, part 1, pp. 656–715, 1949.

[9] H. Wang, X. Zhou, and M. C. Reed, "On the physical layer security in large scale cellular networks," in *Proceedings of the IEEE Wireless Communications & Networking Conference (WCNC '13)*, Shanghai, China, April 2013.

[10] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: a stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2776–2787, 2013.

[11] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, 1996.

[12] A. Sarkar and M. Haenggi, "Secrecy coverage," in *Proceedings of the 44th Asilomar Conference on Signals, Systems and Computers*, pp. 42–46, November 2010.

[13] A. Sarkar and M. Haenggi, "Secrecy coverage, Internet Mathematics," 2012, http://myweb.wwu.edu/sarkara/jgt-revised.pdf.

[14] A. Sarkar and M. Haenggi, "Percolation in the secrecy graph," in *Proceedings of the Information Theory and Applications Workshop (ITA '11)*, San Diego, Calif, USA, February 2011.

[15] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '09)*, pp. 2442–2446, July 2009.

[16] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, 2011.

[17] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, pp. 550–560, 2012.

[18] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, 2012.

[19] N. Marina, T. Stojanovski, and H. V. Poor, "Improvement of information-theoretic secrecy by smart cooperation," in *Proceedings of the Information Theory and Its Applications Workshop (ITA '12)*, La Jolla, Calif, USA, February 2012.

[20] N. Marina, T. Stojanovski, and H. V. Poor, "Increasing the information-theoretic secrecy by cooperative relaying and jamming," in *Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing*, pp. 42–46, October 2012.