### Techniques for enhanced physical-layer security

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

| Citation       | Pinto, P.C., J. Barros, and M.Z. Win. “Techniques for Enhanced Physical-Layer Security.” GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference. 2010. 1-5. Copyright © 2010, IEEE |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| As Published   | http://dx.doi.org/10.1109/GLOCOM.2010.5683460                                                                                                                                                     |
| Publisher      | Institute of Electrical and Electronics Engineers                                                                                                                                                 |
| Version        | Final published version                                                                                                                                                                           |
| Citable link   | http://hdl.handle.net/1721.1/66197                                                                                                                                                                |
| Terms of Use   | Article is made available in accordance with the publisher’s policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.                                        |
Techniques for Enhanced Physical-Layer Security

Pedro C. Pinto, Student Member, IEEE, João Barros, Member, IEEE, and Moe Z. Win, Fellow, IEEE

Abstract—Information-theoretic security—widely accepted as the strictest notion of security—relies on channel coding techniques that exploit the inherent randomness of propagation channels to strengthen the security of communications systems. Within this paradigm, we explore strategies to improve secure connectivity in a wireless network. We first consider the intrinsically secure communications graph (iS-graph), a convenient representation of the links that can be established with information-theoretic security on a large-scale network. We then propose and characterize two techniques—sectorized transmission and eavesdropper neutralization—which are shown to dramatically enhance the connectivity of the iS-graph.

Index Terms—Physical-layer security, wireless networks, secure connectivity, stochastic geometry, random graphs, node degree.

I. INTRODUCTION

Wireless communication is particularly susceptible to eavesdropping due to the broadcast nature of the transmission medium. In current systems, security is addressed above the physical layer using cryptographic protocols (e.g., RSA and AES), which assume that an error-free physical link has already been established. In contrast with this paradigm, it is possible to take advantage of physical-layer techniques to significantly strengthen the security of communication systems. This is the basic principle of information-theoretic security, widely accepted as the strictest notion of security. It relies on channel coding techniques that exploit the inherent randomness of propagation channels to ensure that the transmitted messages cannot be decoded by a malicious eavesdropper.

The basis for information-theoretic security, which builds on the notion of perfect secrecy [1], was laid in [2] and later in [3], [4]. More recently, there has been a renewed interest in information-theoretic security over wireless channels, from the perspective of space-time communications [5], multiple-input multiple-output communications [6]–[10], eavesdropper collusion [11], [12], cooperative relay networks [13], fading channels [14]–[18], strong secrecy [19], [20], secret key agreement [21]–[25], code design [26]–[28], among other topics. A fundamental limitation of this literature is that it only considers scenarios with a small number of nodes. To account for large-scale networks composed of multiple legitimate and eavesdropper nodes, secrecy graphs were introduced in [29] from a geometrical perspective, and in [30] from an information-theoretic perspective. The local connectivity of secrecy graphs was extensively characterized in [31], while the scaling laws of the secrecy capacity were presented in [32], [33]. The feasibility of long-range secure communication was proved in [34], in the context of continuum percolation.

In this paper, we explore strategies to improve secure connectivity in a wireless network. We first consider the intrinsically secure communications graph (iS-graph)—a convenient representation of the links that can be established with information-theoretic security on a large network. We then propose two techniques for improving the connectivity of the iS-graph: (i) sectorized transmission, whereby each legitimate node transmits independently in multiple sectors of the plane (e.g., using directional antennas); and (ii) eavesdropper neutralization, whereby each legitimate node guarantees the absence of eavesdroppers in a surrounding region (e.g., by deactivating such eavesdroppers). We quantify and compare the effectiveness of the proposed techniques in terms of the resulting average node degree.

This paper is organized as follows. Section II describes the system model. Section III proposes and compares techniques for enhancing the secrecy of communication. Section IV provides some numerical results. Section V summarizes important findings.

II. SYSTEM MODEL

A. Wireless Propagation

Given a transmitter node $x_i \in \mathbb{R}^d$ and a receiver node $x_j \in \mathbb{R}^d$, we model the received power $P_{rx}(x_i, x_j)$ associated with the wireless link $\overrightarrow{x_i x_j}$ as

$$ P_{rx}(x_i, x_j) = P \cdot g(x_i, x_j), $$

where $P$ is the transmit power, and $g(x_i, x_j)$ is the power gain of the link $\overrightarrow{x_i x_j}$. The gain $g(x_i, x_j)$ is considered constant (quasi-static) throughout the use of the communications channel, corresponding to channels with a large coherence time. Furthermore, the function $g$ is assumed to satisfy the following conditions, which are typically observed in practice: i) $g(x_i, x_j)$ depends on $x_i$ and $x_j$ only through the link length $|x_i - x_j|_2^2$ ii) $g(r)$ is continuous and strictly decreasing with $r$; and iii) $\lim_{r \to \infty} g(r) = 0$.

B. iS-Graph

Consider a wireless network where the legitimate nodes and the potential eavesdroppers are randomly scattered in

$$ g(r) \triangleq g(x_i, x_j)|_{|x_i - x_j|_2 = r}. $$

With abuse of notation, we write $g(r)$.
space, according to some point processes. The $i\!S$-graph is a convenient representation of the links that can be established with information-theoretic security on such a network.

**Definition 2.1 ($i\!S$-Graph [31]):** Let $\Pi_l = \{x_i\}_{i=1}^\infty \subset \mathbb{R}^d$ denote the set of legitimate nodes, and $\Pi_e = \{e_i\}_{i=1}^\infty \subset \mathbb{R}^d$ denote the set of eavesdroppers. The $i\!S$-graph is the directed graph $G = (\Pi_l, \mathcal{E})$ with vertex set $\Pi_l$ and edge set

$$\mathcal{E} = \{ \overline{x_i x_j} : \mathcal{R}_\ell(x_i, x_j) > 0 \},$$

where $\ell$ is a threshold representing the prescribed infimum secrecy rate for each communication link; and $\mathcal{R}_\ell(x_i, x_j)$ is the maximum secrecy rate (MSR) of the link $\overline{x_i x_j}$, given by

$$\mathcal{R}_\ell(x_i, x_j) = \left[ \log_2 \left( 1 + \frac{P_{rx}(x_i, x_j)}{\sigma_\ell^2} \right) - \log_2 \left( 1 + \frac{P_{rx}(x_i, e^*)}{\sigma_e^2} \right) \right]^+,$$

in bits per complex dimension, where $[x]^+ = \max\{0, x\}$; $\sigma_\ell^2$, $\sigma_e^2$ are the noise powers of the legitimate users and eavesdroppers, respectively; and $e^* = \arg\max_{e_k \in \Pi_e} P_{rx}(x_i, e_k)$. In particular, the average node degrees are given by

$$E\{N_{out}\} = E\{N_{in}\} = \frac{\lambda_l}{\lambda_e}.$$  

**III. Techniques for Enhanced Secure Communication**

In this section, we first characterize the connectivity of the $i\!S$-graph without any enhancement (as introduced in Definition 2.1), and then propose two techniques for improving secure connectivity: sectorized transmission and eavesdropper neutralization. For each strategy, we characterize the average node degree of a typical node in the corresponding enhanced $i\!S$-graph. The average degree is a measure of secure connectivity, and is used in this paper to quantify and compare the effectiveness of each strategy.

**A. Secure Communication Without Enhancement**

We start by characterizing secure connectivity in the $i\!S$-graph when no particular strategy is used.

**Theorem 3.1 (No Enhancement):** The out-degree $N_{out}$ of a typical node in the Poisson $i\!S$-graph has the following geometric probability mass function (PMF)

$$p_{N_{out}}(n) = \left( \frac{\lambda_l}{\lambda_l + \lambda_e} \right)^n \left( \frac{\lambda_e}{\lambda_l + \lambda_e} \right), \quad n \geq 0.$$  

In particular, the average node degrees are given by

$$E\{N_{out}\} = E\{N_{in}\} = \frac{\lambda_l}{\lambda_e}.$$  

**Proof:** See [29], [30].

We observe that in the $i\!S$-graph without enhancement, even a small density of eavesdroppers is enough to significantly disrupt connectivity. For example, if the density of eavesdroppers is half the density of legitimate nodes, then the average node degree is only $\frac{\lambda_l}{\lambda_e} = 2$. In what follows, we propose techniques that achieve an average degree higher than $\frac{\lambda_l}{\lambda_e}$.

**B. Secure Communication With Sectorized Transmission**

We have so far assumed that the legitimate nodes employ omnidirectional antennas, distributing power equally among all directions in space. We now let each legitimate node transmit independently in $L$ sectors of the plane, with $L \geq 1$. This can be accomplished, for example, through the use of $L$ directional antennas. Our goal is to characterize the impact of the number of sectors $L$ on the local connectivity of the resulting $i\!S$-graph.

With each node $x_i \in \Pi_l$, we associate $L$ transmission sectors $\{S_i^{(l)}\}_{l=1}^L$, defined as

$$S_i^{(l)} \triangleq \left\{ z \in \mathbb{R}^2 : \phi_i + (l-1) \frac{2\pi}{L} < \angle \overline{x_i z} < \phi_i + l \frac{2\pi}{L} \right\}.$$ 

We analyze the properties of a typical node, a notion which is made precise in [37, Sec. 4.4] using Palm theory. Specifically, Slivnyak’s theorem states that the properties observed by a typical legitimate node $x \in \Pi_l$ are the same as those observed by node 0 in the process $\Pi_l \cup \{0\}$. Informally, a typical node of $\Pi_l$ is one that is uniformly picked from a finite region expanding to $\mathbb{R}^2$. 

---

3This definition uses strong secrecy as the condition for information-theoretic security. See [19], [31, Sec. II-B] for more details.

4Note that by setting $\ell = 0$ we are considering the existence of secure links, in the sense that an edge $\overline{x_i x_j}$ is present iff $\mathcal{R}_\ell(x_i, x_j) > 0$. The general case of non-zero secrecy rate threshold, $\ell > 0$, and unequal noise powers, $\sigma_\ell^2 \neq \sigma_e^2$, can still be considered (see [31, Sec. III-E] for an analysis) but does not provide as many insights.

5We analyze the properties of a typical node, a notion which is made precise in [37, Sec. 4.4] using Palm theory. Specifically, Slivnyak’s theorem states that the properties observed by a typical legitimate node $x \in \Pi_l$ are the same as those observed by node 0 in the process $\Pi_l \cup \{0\}$. Informally, a typical node of $\Pi_l$ is one that is uniformly picked from a finite region expanding to $\mathbb{R}^2$. 

---

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.
information-theoretic security to $N_{\text{out}}(l)$ if and only if $x_j$ is closer to $x_i$ than any other eavesdropper that has not been neutralized. In this case, the eavesdropper in sector $S_j$ can only hear the transmissions inside sector $S_j$. However, if we allow independent transmissions in four non-overlapping sectors, that same eavesdropper can only hear the transmissions inside sector $S_j$. Thus, even though node $0$ is out-isolated with respect to sector $S_j$, it may still communicate securely with some legitimate nodes inside sectors $S(l)$, $S(2)$, and $S(3)$. Lastly, note that for $L = 1$ (i.e., no enhancement), Theorem 3.2 reduces to Theorem 3.1 as expected.

C. Secure Communication With Eavesdropper Neutralization

In some scenarios, each legitimate node may be able to physically inspect its surroundings and deactivate the eavesdroppers falling inside some neutralization region. Our goal is to characterize the impact of such region on the local connectivity of the resulting $iS$-graph.

With each node $x_i \in \Pi_l$, we associate a neutralization region $\Theta_l$ inside which all eavesdroppers have been deactivated. The total neutralization region $\Theta$ can then be seen as a Boolean model with points $\{x_i\}$ and associated sets $\{\Theta_i\}$, i.e., [37]

$$\Theta = \bigcup_{i=1}^{\infty} (x_i + \Theta_l).$$

Since the eavesdroppers inside $\Theta$ have been deactivated, the effective eavesdropper process after neutralization is $\Pi_e \cap \Theta$, and hence $\Theta$ denotes the complement of $\Theta$. The resulting $iS$-graph with neutralization, $G_{\Theta} = \{\Pi_{(x_l)}, \mathcal{E}_{\Theta}\}$, has an edge set given by

$$\mathcal{E}_{\Theta} = \left\{ \frac{x_i x_j}{|x_i - x_j|} : |x_i - x_j| < |x_i - e^*|, e^* = \arg\min_{e_k \in \Pi_{(x_l)}/\Theta} |x_i - e_k| \right\},$$

i.e., the secure link $\frac{x_i x_j}{|x_i - x_j|}$ exists if and only if $x_j$ is closer to $x_i$ than any other eavesdropper that has not been neutralized. In the following, we consider the case of a circular neutralization set, i.e., $\Theta_i = B_0(\rho)$, where $\rho$ is a deterministic neutralization radius, and denote the corresponding graph by $G_{\rho}$.

**Theorem 3.3 (Eavesdropper Neutralization):** For the enhanced Poisson $iS$-graph $G_{\rho}$ with neutralization radius $\rho$, determine the PMF of $N_{\text{out}}(l)$, we use the fact that $\{(R_{i,e})_j^2\}_{j=1}^{\infty}$ and $\{(R_{i,e})_j^2\}_{j=1}^{\infty}$ are homogeneous Poisson processes with rates $\frac{\lambda_0}{\lambda_e + \lambda_e}$ and $\frac{\lambda_0}{\lambda_e + \lambda_e}$, respectively (by the mapping theorem [35, Sec. 2.3]). Following steps analogous to the proof of [30, Thm. 3.1], it is easy to show that $N_{\text{out}}(l)$ has a geometric PMF given by $p_{N_{\text{out}}(l)}(n) = \rho^n(1 - \rho)$, $n \geq 0$, with $\rho = \frac{\lambda_0}{\lambda_e + \lambda_e}$. Now, since the RVs $\{N_{\text{out}}(l)\}$ are IID in $l$, the total out-degree $N_{\text{out}}$ has a negative binomial PMF with $L$ degrees of freedom and the same parameter $\rho$, i.e., $p_{N_{\text{out}}}(n) = (\frac{L + n - 1}{L - 1})\rho^n(1 - \rho)^L$, $n \geq 0$, with $\rho = \frac{\lambda_0}{\lambda_e + \lambda_e}$. This is the result in (4), from which (5) follows trivially.

We conclude that the average node degree increases *linearly* with the number of sectors $L$, and hence sectorized transmission is an effective technique for enhancing the secrecy of communications. Figure 2 provides an intuitive understanding of why sectorization works. Specifically, if there was no sectorization, node 0 would be out-isolated, due to the close proximity of the eavesdropper in sector $S_j$. However, if we allow independent transmissions in four non-overlapping sectors, that same eavesdropper can only hear the transmissions inside sector $S_j$. Thus, even though node 0 is out-isolated with respect to sector $S_j$, it may still communicate securely with some legitimate nodes inside sectors $S(l)$, $S(2)$, and $S(3)$. Lastly, note that for $L = 1$ (i.e., no enhancement), Theorem 3.2 reduces to Theorem 3.1 as expected.

This is because the sectors $\{S(l)\}_{l=1}^{L}$ correspond to an equipartition of $\mathbb{R}^2$, and the processes $\Pi_{(x_l)}, \Pi_e$ are homogeneous Poisson.
Fig. 3. Let \( \lambda \) be the average node degrees of a typical node are lower-bounded by
\[
\mathbb{E}\{N_{out}\} = \mathbb{E}\{N_{in}\} \geq \frac{\lambda}{\lambda E} \left( \pi \lambda e \rho^2 + e^{\pi \lambda \rho^2} \right). \tag{6}
\]

Proof: We consider the process \( \Pi_\ell \cup \{0\} \) obtained by adding a legitimate node to the origin of the coordinate system, and denote the out-degree of node 0 by \( N_{out} \), as depicted in Fig. 3. Let \( R_{e,1} \triangleq \min_{e_k \in \Pi_\ell \cap \mathbb{R}^2} |e_k| \) be the random distance between the first non-neutralized eavesdropper and the origin. Noting that
\[
N_{out} = \sum_{x_i \in \Pi_\ell} 1\{|x| < R_{e,1}\} = \int_{\mathbb{R}^2} 1\{|x| < R_{e,1}\} \Pi_\ell(dx),
\]
we can use Fubini’s theorem to write
\[
\mathbb{E}\{N_{out}\} = \lambda \int_{\mathbb{R}^2} \mathbb{P}_x\{|x| < R_{e,1}\} dx
= \lambda \pi \rho^2 + \lambda \int_{D(0, \infty)} \mathbb{P}_x\{|x| < R_{e,1}\} dx, \tag{7}
\]
where \( D(a, b) \triangleq \{x \in \mathbb{R}^2 : a \leq |x| \leq b\} \) denotes the annulus centered at the origin, with inner radius \( a \) and outer radius \( b \); and \( \mathbb{P}_x\{\cdot\} \) is the Palm probability associated with point \( x \) of process \( \Pi_\ell \).\(^8\) Appendix A shows that the integrand above satisfies
\[
\mathbb{P}_x\{|x| < R_{e,1}\} \geq \exp\left(-\pi \lambda e^{-\lambda \pi \rho^2}\{|x|^2 - \rho^2\}\right). \tag{8}
\]
Replacing (8) into (7), we have
\[
\mathbb{E}\{N_{out}\} \geq \lambda \pi \rho^2 + \lambda \int_{D(0, \infty)} \exp\left(-\pi \lambda e^{-\lambda \pi \rho^2}\{|x|^2 - \rho^2\}\right) dx
= \lambda \pi \rho^2 + \lambda \lambda E e^{\pi \lambda \rho^2}.
\]
Rearranging terms and noting that \( \mathbb{E}\{N_{out}\} = \mathbb{E}\{N_{in}\} \), we obtain (6).

We conclude that the average node degree increases at a rate that is at least exponential with the neutralization radius \( \rho \), making eavesdropper neutralization an effective technique for enhancing the secrecy of communications.

IV. NUMERICAL RESULTS

Figure 4 illustrates the effectiveness of eavesdropper neutralization in enhancing secure connectivity. In particular, it plots the average node degree versus the neutralization radius \( \rho \), for various values of \( \lambda_e \). We observe that the analytical lower-bound for \( \mathbb{E}\{N_{out}\} \) given in (6) is very close to the actual value of \( \mathbb{E}\{N_{out}\} \) obtained through Monte Carlo simulation. The lower-bound becomes tight in the following two extreme cases:

1. \( \rho = 0 \): This corresponds to the case of no enhancement, so from (3) we have \( \mathbb{E}\{N_{out}\} = \frac{\lambda}{\lambda E} \). Since the bound in (6) also equals \( \frac{\lambda}{\lambda E} \) for \( \rho = 0 \), it is tight.
2. \( \lambda_e \to \infty \): In the limit, at least one eavesdropper will fall almost surely inside the annulus \( D(\rho, \rho + \epsilon) \), for any \( \epsilon > 0 \). As a result, \( \mathbb{E}\{N_{out}\} \) approaches the average number of legitimate nodes inside the ball \( B_0(\rho) \), i.e., \( \lambda_\ell \pi \rho^2 \). Since the bound in (6) also approaches \( \lambda_\ell \pi \rho^2 \) as \( \lambda_e \to \infty \), it is asymptotically tight.

V. CONCLUSIONS

In this paper, we proposed two techniques shown to dramatically enhance the connectivity of the iS-graph: sectorized transmission and eavesdropper neutralization. We proved that if each legitimate node is able to transmit independently in \( L \) sectors of the plane, the average node degree increases linearly with \( L \). On the other hand, if each legitimate node is able to neutralize all eavesdroppers within a radius \( \rho \), the average degree increases at least exponentially with \( \rho \). We are hopeful that further efforts will provide an understanding of how long-range secure communication is improved by the two proposed strategies. For example, the effect of \( L \) and \( \rho \) on the critical densities for continuum percolation is still unknown, as is their effect on the secrecy capacity scaling laws.

---

\(^8\)Informally, the Palm probability \( \mathbb{P}_x\{\cdot\} \) can be interpreted as the conditional probability \( \mathbb{P}\{\cdot | x \in \Pi_\ell\} \). Since the conditioning event has probability zero, such conditional probability is ambiguous without further explanation. Palm theory makes this notion mathematically precise (see [37, Sec. 4.4] for a detailed treatment).
APPENDIX A 
DERIVATION OF (8)

Because $\Pi_\ell$ is a Poisson process, the Palm probability $\mathbb{P}_x\{ |x| < R_{\ell,1} \}$ in (7) can be computed using Slivnyak’s theorem by adding a legitimate node at location $x$ to $\Pi_\ell$. For a fixed $x \in \mathcal{D}(\rho, \infty)$, we can thus write

$$
\mathbb{P}_x\{ |x| < R_{\ell,1} \} = \mathbb{P}_x\{ \Pi_\ell(\Theta \cap \mathcal{D}(\rho, |x|)) \} = 0 \}
\geq \mathbb{E}_\Theta \{ \exp(-\lambda \mathbb{A}(\Theta \cap \mathcal{D}(\rho, |x|)) \}
\geq \exp(-\lambda \mathbb{E}_\Theta \{ \mathbb{A}(\Theta \cap \mathcal{D}(\rho, |x|)) \})
$$

(9)

(10)

where $\mathbb{A}(\mathcal{R})$ denotes the area of the arbitrary region $\mathcal{R}$. Equation (9) follows from conditioning on $\Theta$, and using the fact that $\Pi_\ell$ and $\Theta$ are independent. Equation (10) follows from Jensen’s inequality. The term inside the exponential in (10) corresponds to the average area of a random shape, and can be computed using Fubini’s theorem as

$$
\mathbb{E}_\Theta \{ \mathbb{A}(\Theta \cap \mathcal{D}(\rho, |x|)) \}
= \mathbb{E}_\Theta \left\{ \int_{\mathbb{R}^2} \mathbb{1}_{y \in \Theta \cap \mathcal{D}(\rho, |x|)} dy \right\}
= \int_{\mathcal{D}(\rho, |x|)} \mathbb{P}(y \in \Theta) dy
= \int_{\mathcal{D}(\rho, |x|)} \mathbb{P}(\Pi_\ell(\mathcal{B}(\rho)) = 0) dy
= \int_{\mathcal{D}(\rho, |x|)} e^{-\lambda \pi \rho^2} dy
= \pi (|x|^2 - \rho^2) e^{-\lambda \pi \rho^2}
$$

Replacing (11) into (10), we obtain the desired inequality in (8).

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 29, pp. 656–715, 1949.
[2] A. D. Wyner, “The Wire-Tap Channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1367, October 1975.
[3] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, 1978.
[4] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, July 1978.
[5] A. Hero, “Secure space-time communication,” IEEE Transactions on Information, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[6] R. Negi and S. Goel, “Secret communication using artificial noise,” in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, ON, July 2008, pp. 2217–2221.
[7] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in Proc. IEEE Int. Symp. on Inf. Theory, Adelaide, Australia, Sept. 2005, pp. 2152–2155.
[8] P. Gopala, L. Lai, and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” arxiv preprint cs.IT/0610103, 2006.
[9] Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” Proc. Allerton Conf. on Communication, Control and Computing, pp. 841–848, Sept. 2006.
[10] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, 2008.
[11] S. Goel and R. Negi, “Secret communication in presence of colluding eavesdroppers,” in Proc. Military Commun. Conf., Oct. 2005, pp. 1501–1506.
[12] P. C. Pinto, J. O. Barros, and M. Z. Win, “Wireless physical-layer security: The case of colluding eavesdroppers,” in Proc. IEEE Int. Symp. on Inf. Theory, Seoul, South Korea, July 2009, pp. 2442–2446.
[13] E. Ekrem and S. Ulukus, “Secrecy in cooperative relay broadcast channels,” in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, ON, July 2008, pp. 2217–2221.
[14] F. Gomara, L. Lai, and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” arxiv preprint cs.IT/0610103, 2006.
[15] Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” Proc. Allerton Conf. on Communication, Control and Computing, pp. 841–848, Sept. 2006.
[16] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, 2008.
[17] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” IEEE Trans. Inf. Theory, vol. 54, pp. 2470–2492, June 2008.
[18] U. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” Eurocrypt 2000, Lecture Notes in Computer Science, vol. 1807, pp. 351+, 2000.
[19] J. Barros and M. Bloch, “Strong secrecy for wireless channels,” in Proc. International Conf. on Inf. Theor. Security, Calgary, Canada, Aug. 2008.
[20] U. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.
[21] A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, “LDPC-based secret key agreement over the gaussian wiretap channel,” in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, Canada, July 2008.
[22] Y. Liang, H. V. Poor, and S. Shamai, “On the Secrecy Capacity of Fading Channels,” IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[23] J. Barros and M. Bloch, “Strong secrecy for wireless channels,” in Proc. International Conf. on Inf. Theor. Security, Calgary, Canada, Aug. 2008.
[24] U. Maurer, “Secret key agreement from correlated source outputs using low density parity check matrices,” IEEE Trans. Fund. of Elec. Comm. Comp., vol. E9-A, no. 7, pp. 2036–2046, July 2006.
[25] M. Haenggi, “The secrecy graph and some of its properties,” in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, Canada, July 2008.
[26] P. C. Pinto, J. O. Barros, and M. Z. Win, “Physical-layer security in stochastic wireless networks,” in Proc. IEEE Int. Conf. on Commun. Systems, Guangzhou, China, Nov. 2008, pp. 974–979.
[27] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, “Applications of LDPC codes to the wiretap channel,” IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[28] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, “Secure nested codes for type II wiretap channels,” in Proc. IEEE Inf. Theory Workshop, Tahoe City, CA, Sept. 2007, pp. 337–342.
[29] J. Muramatsu, “Secret key agreement from correlated source outputs using low density parity check matrices,” IEICE Trans. Fund. of Elec. Comm. Comp., vol. E99-A, no. 7, pp. 2036–2046, July 2006.
[30] P. C. Pinto, J. O. Barros, and M. Z. Win, “Secrecy capacity in stochastic wireless networks,” in Proc. IEEE Int. Conf. on Commun. Systems, Guangzhou, China, Nov. 2008, pp. 974–979.
[31] ———, “Secret communication in stochastic wireless networks,” IEEE Trans. Inf. Theory, pp. 1–59, 2009, submitted for publication, preprint available on arXiv:1001.3697.
[32] Y. Liang, H. V. Poor, and L. Ying, “Secrecy throughput of MANETs with malicious nodes,” in Proc. IEEE Int. Symp. on Inf. Theory, June 2009, pp. 1189–1193.
[33] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, “On secrecy capacity scaling in wireless networks,” in Inf. Theory and Applications Workshop, San Diego, CA, Feb. 2010, pp. 1–4.
[34] P. C. Pinto and M. Z. Win, “Continuum percolation in the intrinsically securely communications graph,” in Proc. IEEE Int. Symp. on Inf. Theory and Its Applications, Taichung, Taiwan, Oct. 2010, pp. 1–6.
[35] M. Haenggi, P. Gopala, L. Lai, and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” IEEE J. Sel. Areas Commun., vol. 27, no. 7, pp. 1029–1046, 2009.
[36] D. Stoyan, W. S. Kendall, and J. Mecke, Stochastic geometry and its applications. John Wiley & Sons, 1995.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.