Wireless physical-layer security: The case of colluding eavesdroppers

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

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1109/ISIT.2009.5206050">http://dx.doi.org/10.1109/ISIT.2009.5206050</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/60236">http://hdl.handle.net/1721.1/60236</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>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.</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td></td>
</tr>
</tbody>
</table>
Abstract—We consider the fundamental security limits of stochastic wireless networks in the presence of colluding eavesdroppers. By establishing a direct connection with the single-input multiple-output (SIMO) Gaussian wiretap channel, we are able to provide a complete characterization of the secrecy capacity for the case in which the eavesdroppers are scattered according to a spatial Poisson process. Our analysis, which includes the probabilities of existence and outage of secrecy capacity, helps clarify how the spatial density of eavesdroppers can jeopardize the success of wireless physical-layer security based on information-theoretic principles.

Index Terms—Information-theoretic security, wireless channels, secrecy capacity, colluding eavesdroppers, stochastic geometry.

I. INTRODUCTION

Although much has been achieved in terms of securing the higher layers of the classical protocol stack, protecting the physical layer of wireless networks from one or multiple eavesdroppers remains a formidable task. Due to the properties of the physical medium, any unauthorized receiver located within the transmission range is capable of observing the signals sent by the legitimate transmitters. Moreover, the attacker is free to combine its own observations with those of other eavesdroppers, thus improving its reception by means of cooperative inference. On a more positive tone, recent results in information theory indicate that the physical properties of wireless channels, such as multipath fading, can be used effectively to complement the levels of secrecy attained by means of classical cryptographic primitives.

The theoretical foundation for physical-layer security over noisy channels, which builds on the notion of perfect secrecy [1], was laid in [2] and later in [3]. More recently, space-time signal processing techniques for secure communication over wireless links appeared in [4], and the secrecy capacity of various single-input multiple-output (SIMO) fading channels was established in [5]. The concept of outage secrecy capacity of slow fading channels was presented in detail in [6], whereas the ergodic secrecy capacity of fading channels was derived in [7], [8]. The presence of colluding eavesdroppers is considered in [9], but restricting its attention to a fixed number of eavesdroppers placed at the same spatial location. The secrecy properties of stochastic wireless networks are discussed in [10], [11], for the case of non-colluding eavesdroppers.

Intrigued by the fundamental limits of physical-layer security in wireless networks with multiple colluding eavesdroppers, we address the issue of how the spatial distribution of the eavesdroppers and the propagation characteristics of the channel ultimately determine the achievable secrecy rates. In large-scale wireless networks, the spatial distribution of the nodes can be modeled either deterministically or stochastically. Deterministic models include square, triangular, and hexagonal lattices in the two-dimensional plane [12], [13], which are applicable when the location of the nodes in the network is known exactly or is constrained to a regular structure. However, in many ad-hoc scenarios, only a statistical description of the location of the nodes is available, and thus a stochastic spatial model should be employed. In particular, the homogeneous Poisson point process [14] is a natural model when all the points in a region are equally likely possibilities for the location of a node. The Poisson process has been successfully used in the context of wireless networks, to analyze network interference [15], [16], connectivity and coverage [17], [18], routing [19], and sensor cooperation [20], among other topics.

The main contributions of this paper are as follows:

- **Secrecy capacity in the presence of colluding eavesdroppers:** After establishing the equivalence between communication in the presence of colluding eavesdroppers and the SIMO Gaussian wiretap channel, we obtain an expression for the corresponding secrecy capacity, when the eavesdroppers are scattered according to an arbitrary spatial process.
- **Probabilistic characterization of the secrecy capacity:** For the case where the eavesdroppers are scattered according to a spatial Poisson process, we provide the cumulative distribution function (c.d.f.) of the corresponding secrecy capacity.
- **Existence and outage of secrecy capacity:** We present expressions for the probabilities of existence and outage of the secrecy capacity, in the presence of a Poisson field of colluding eavesdroppers.

The remainder of the paper is organized as follows. Section II describes the system model. Section III considers the secrecy capacity for an arbitrary spatial process of eavesdroppers. Section IV characterizes the distribution of the secrecy capacity when the eavesdroppers are spatially distributed according to a Poisson process. Section V analyzes the corresponding existence and outage of secrecy capacity. Section VI presents
We consider that Alice sends a symbol \( x \) with power constraint \( P \), and the output of the SIMO wiretap channel is the collection of signals received by all the eavesdroppers. The noise is represented by the noise vectors \( \mathbf{w}_M \in \mathbb{C}^m \) and \( \mathbf{w}_E \in \mathbb{C}^n \), considered mutually independent and Gaussian distributed with zero mean and non-singular covariance matrices \( \Sigma_M \) and \( \Sigma_E \), respectively.

The system of Fig. 2 can then be summarized as

\[
\begin{align*}
\mathbf{y}_M &= \mathbf{h}_M x + \mathbf{w}_M \\
\mathbf{y}_E &= \mathbf{h}_E x + \mathbf{w}_E.
\end{align*}
\]

(1)

The general SIMO system in Fig. 2 reduces to the scenario in Fig. 1 by setting \( \mathbf{h}_M = 1/r_M^b \mathbf{I}_M \), \( \mathbf{h}_E = \mathbf{I}_E \), \( \Sigma_M = W_M \mathbf{I}_M \), and \( \Sigma_E = W_E \mathbf{I}_E \), where \( W_M \) and \( W_E \) are the noise powers of the legitimate and eavesdropper receivers, respectively, and \( \mathbf{I}_n \) is the \( n \times n \) identity matrix.

### III. Secrecy Capacity in the Presence of Colluding Eavesdroppers

In this section, we determine the secrecy capacity of the legitimate link, in the presence of colluding eavesdroppers scattered in the plane according to an arbitrary spatial process. The result is given by following theorem.

**Theorem 3.1**: For a given realization of the arbitrary eavesdropper process \( \Pi_E \), the secrecy capacity of the legitimate link is given by

\[
C_s = \max \left\{ \log_2 \left( 1 + \frac{P}{r_M^b W_M} \right) - \log_2 \left( 1 + \frac{P_E}{W_E} \right) , 0 \right\},
\]

(2)

in bits per complex dimension, where \( P_E \) is the aggregate power received by all the eavesdroppers,

\[
P_E = \sum_{i=1}^{\infty} \frac{P}{r_i^b}.
\]

(3)

**Proof**: Writing the maximum-a-posteriori rule for the main channel in Fig. 2, it can be shown that a sufficient statistic to estimate \( x \) from \( \mathbf{y}_M = \mathbf{h}_M^\dagger \Sigma_M^{-1} \mathbf{y}_M \), and similarly for the eavesdroppers’ channel [22]. Since sufficient statistics preserve mutual information, we can equivalently express (1) in terms of sufficient statistics, for the purpose of determining the secrecy capacity. Thus, by left-multiplying

---

1. Note that the amplitude loss exponent is \( b \), while the corresponding power loss exponent is \( 2b \).
2. We use boldface letters to denote vectors and matrices.
3. We use \( \dagger \) to denote the conjugate transpose operator.
each side of the equations by the corresponding term $h^\top \Sigma^{-1}$, we obtain
\[
\begin{align*}
\tilde{y}_M &= \tilde{h}_M x + \tilde{w}_M, \\
\tilde{y}_E &= \tilde{h}_E x + \tilde{w}_E,
\end{align*}
\]
where
\[
\begin{align*}
\tilde{h}_M &= h_M^1 \Sigma_M^{-1} h_M, \\
\tilde{h}_E &= h_E^1 \Sigma_E^{-1} h_E \\
\tilde{w}_M &\sim \mathcal{N}_c(0, \tilde{h}_M) \\
\tilde{w}_E &\sim \mathcal{N}_c(0, \tilde{h}_E),
\end{align*}
\]
and $\tilde{w}_M$ is independent of $\tilde{w}_E$. This (complex) scalar description corresponds to the Gaussian wiretap channel introduced in [23]. If $C_M$ and $C_E$ denote the capacities of the main and eavesdroppers channels, respectively, we know that the secrecy capacity $C_s$ of the main channel for some realization of the channels $h_M$ and $h_E$ is given by
\[
C_s = C_M - C_E
= \max \left\{ \log_2 \left( 1 + \frac{\tilde{h}_M^2 P}{h_M^2} \right) - \log_2 \left( 1 + \frac{\tilde{h}_E^2 P}{h_E^2} \right), 0 \right\}.
\]
Setting $h_M = 1/\sqrt{\lambda^b}$, $h_E = [1/\Gamma_1, 1/\Gamma_2, \ldots]^T$, $\Sigma_M = W_M I_1$, and $\Sigma_E = W_E \Sigma_{\infty}$, (4) reduces to
\[
C_s = \max \left\{ \log_2 \left( 1 + \frac{P}{\tilde{h}_M^2 \Sigma_{\infty}^{-1} h_E P} \right), 0 \right\}.
\]
where $P_E = \sum_{i=1}^{\infty} P_{i \Gamma_{i}}$ is the aggregate power received by all the eavesdroppers. This is the result in (2) and the proof is concluded.  \hfill \Box

IV. PROBABILISTIC CHARACTERIZATION OF THE SECRECY CAPACITY

Theorem 3.1 is valid for an arbitrary spatial process $\Pi_E$, deterministic or stochastic. In the latter case, the secrecy capacity $C_s$ of the main channel in (2) is a random variable (r.v.), since it is a function of the random eavesdropper distances $\{\Gamma_i\}_{i=1}^{\infty}$. In the rest of the paper, we analyze the case where $\Pi_E$ is a homogeneous Poisson process in the two-dimensional plane. Typically, the eavesdropper positions are unknown a priori, so we may as well treat them as completely random according to a spatial Poisson process. Then, the probability $P\{n \in \mathcal{R}\}$ of $n$ eavesdroppers being inside a region $\mathcal{R}$ (not necessarily connected) depends only on the total area $A$ of the region, and is given by [14]
\[
P\{n \in \mathcal{R}\} = \frac{(\lambda_E A)^n}{n!} e^{-\lambda_E A}, \quad n \geq 0,
\]
where $\lambda_E$ is the (constant) spatial density of eavesdroppers, in nodes per unit area. The following theorem characterizes the distribution of the secrecy capacity in this scenario.

**Theorem 4.1:** If $\Pi_E$ is a Poisson process with density $\lambda_E$, the secrecy capacity $C_s$ of the main channel is a r.v. whose c.d.f. $F_{C_s}(c)$ is given by
\[
F_{C_s}(c) = \begin{cases} 
0, & c < 0, \\
1 - F_{P_E} \left( \frac{(\pi \lambda_E \Gamma)^{2-1}}{(\pi \lambda_E \Gamma_{i+1})^{2-1}} \right), & 0 \leq c < C_M, \\
1, & c \geq C_M,
\end{cases}
\]
where $C_M = \log_2 \left( 1 + \frac{P}{\pi \lambda_E \Gamma} \right)$ is the capacity of the main channel; $C_{\alpha}$ is defined as
\[
C_{\alpha} = \frac{1 - \alpha}{\Gamma(2 - \alpha) \cos(\pi \alpha /2)},
\]
with $\Gamma(\cdot)$ denoting the gamma function; and $F_{P_E}(\cdot)$ is the c.d.f. of a stable r.v. $P_E$, with parameters $b > 1$.

**Proof:** The secrecy capacity $C_s$ of the main channel in (2) is a function of the r.v. $P_E$, and is therefore also random. In [15], we show that the characteristic function of $P_E$ in (3) has the form
\[
\phi_{P_E}(w) = \exp \left( -|w|^\alpha \left[ 1 - j \beta \text{sign}(w) \tan \left( \frac{\pi \alpha}{2} \right) \right] \right),
\]
where $\alpha = \frac{1}{b}$, $\beta = 1$, $\gamma = \pi \lambda_E C_{1/b}^{1/b}$, and $b > 1$. R.V.'s with such characteristic function belong to the class of skewed stable distributions [24]. Stable laws are a direct generalization of Gaussian distributions, and include other densities with heavier (algebraic) tails. They share many properties with Gaussian distributions, namely the stability property and the generalized central limit theorem. Equations (9)-(10) can be succinctly expressed as
\[
P_E \sim S \left( \alpha = \frac{1}{b}, \beta = 1, \gamma = \pi \lambda_E C_{1/b}^{1/b} \right),
\]
defining the normalized stable r.v. $P_E = P_E \gamma^{-1/b} = \frac{P_E}{\pi \lambda_E C_{1/b}^{1/b}}$, we have that $\tilde{P}_E \sim S \left( \frac{1}{b}, 1, 1 \right)$ from the scaling property [24]. In general, the c.d.f. $F_{P_E}(\cdot)$ cannot be expressed in closed form except in the case where $b = 2$, which is analyzed in Section VI. However, the characteristic function of $\tilde{P}_E$ has the simple form of $\phi_{\tilde{P}_E}(w) = \exp \left( -|w|^{1/b} \left[ 1 - j \text{sign}(w) \tan \left( \frac{\pi \alpha}{2} \right) \right] \right)$, and thus $F_{\tilde{P}_E}(\cdot)$ can be expressed as
\[
\phi(w) = \exp \left( -|w|^{1/b} \left[ 1 - j \beta \text{sign}(w) \tan \left( \frac{\pi \alpha}{2} \right) \right] \right), \quad \alpha \neq 1,
\]
\[
\exp \left( -|w|^{1/b} \left[ 1 + j \frac{\pi \alpha}{2} \beta \text{sign}(w) \ln |w| \right] \right), \quad \alpha = 1.
\]
always be expressed in the integral and computed numerically.

Using (2), we can now express \( F_{C_s}(c) \) in terms of \( F_{\tilde{P}_E}(\cdot) \), for \( 0 \leq c < C_M \), as

\[
F_{C_s}(c) = \Pr \{ C_s \leq c \} = \Pr \left\{ \log_2 \left( 1 + \frac{P}{r_M^2 W_M} \right) - \log_2 \left( 1 + \frac{P_{\tilde{E}}}{W_{\tilde{E}}} \right) \leq c \} = 1 - \Pr \left\{ P_{\tilde{E}} \leq W_{\tilde{E}} \left[ \left( 1 + \frac{P}{r_M^2 W_M} \right) 2^{-c} - 1 \right] \right\} = 1 - F_{\tilde{P}_E} \left( \frac{\left( 1 + \frac{P}{r_M^2 W_M} \right) 2^{-c} - 1}{\pi \lambda E C_1/b + \frac{P}{W_{\tilde{E}}}} \right).
\]

In addition, \( F_{C_s}(c) = 0 \) for \( c < 0 \) and \( F_{C_s}(c) = 1 \) for \( c \geq C_M \), since the r.v. \( C_s \) in (2) satisfies \( 0 \leq C_s \leq C_M \), i.e., the secrecy capacity of the main link in the presence of colluding eavesdroppers is a positive quantity which cannot be greater that the secrecy capacity of the main link in the absence of eavesdroppers. This is the result in (6) and the proof is complete.

V. Existence and Outage of Secrecy Capacity

Based on the results of Section IV, we now obtain the probabilities of existence and outage of the secrecy capacity, in the presence of a Poisson field of colluding eavesdroppers. The following corollary provides such probabilities.

**Corollary 5.1:** If \( \Pi_{E} \) is a Poisson process with density \( \lambda_E \), the probability of existence of a non-zero secrecy capacity, \( p_{\text{exist}} = \Pr \{ C_s > 0 \} \), is given by

\[
p_{\text{exist}} = F_{\tilde{P}_E} \left( \frac{W_{\tilde{E}}}{(\pi \lambda E)^2 C_1/b + W_{\tilde{E}}} \right), \quad (12)
\]

and the probability of an outage in secrecy capacity, \( p_{\text{outage}}(R_s) = \Pr \{ C_s < R_s \} \) for some target secrecy rate \( R_s > 0 \), is given by

\[
p_{\text{outage}}(R_s) = \begin{cases} 1 - F_{\tilde{P}_E} \left( \frac{\left( 1 + \frac{P}{r_M^2 W_M} \right) 2^{-R_s} - 1}{(\pi \lambda E C_1/b + P_{\tilde{E}}/W_{\tilde{E}})} \right), & 0 < R_s < C_M, \\ 1, & R_s \geq C_M, \end{cases} \quad (13)
\]

where \( C_M = \log_2 \left( 1 + \frac{P}{r_M^2 W_M} \right) \) is the capacity of the main channel; and \( F_{\tilde{P}_E} \) is the c.d.f. of the normalized stable r.v. \( \tilde{P}_E \), with parameters given in (8).

**Proof:** The expressions for \( p_{\text{exist}} \) and \( p_{\text{outage}}(R_s) \) follow directly from (6).

VI. Case Study

We now illustrate the results obtained in the previous sections with a simple case study. We consider the case where \( W_M = W_{\tilde{E}} = W \), i.e., the main link and the eavesdroppers are subject to the same noise power, introduced by the electronics of the respective receivers. Furthermore, we consider that the amplitude loss exponent is \( b = 2 \), in which case the c.d.f. of \( \tilde{P}_E \) can be expressed in closed form as \( F_{\tilde{P}_E}(x) = \text{erfc}(1/\sqrt{2x}), x \geq 0 \). The c.d.f. of \( C_s \) in (6) reduces to

\[
F_{C_s}(c) = \begin{cases} 0, & c < 0, \\ \text{erfc} \left( \frac{\pi \lambda E C_1/(b + 1)}{(1 + r_M^2 W) 2^{-c} - 1} \right), & 0 \leq c < C_M, \\ 1, & c \geq C_M. \end{cases}
\]

In addition, (12) and (13) reduce, respectively, to

\[
p_{\text{exist}} = \text{erfc} \left( \frac{\pi \lambda E C_1/(b + 1)}{1 + r_M^2 W} \right) C_1/(b + 1), \quad (15)
\]

and

\[
p_{\text{outage}}(R_s) = \begin{cases} \text{erfc} \left( \frac{\pi \lambda E C_1/(b + 1)}{1 + r_M^2 W} \right) C_1/(b + 1), & 0 < R_s < C_M, \\ 1, & R_s \geq C_M. \end{cases}
\]

Figures 3 and 4 quantify, respectively, the c.d.f. and p.d.f. of the secrecy capacity \( C_s \) of the main link, for the considered case study. We observe that \( C_s \) is a positive quantity which cannot be greater than the secrecy capacity \( C_M \) of the main link in the absence of eavesdroppers, which in this case is \( C_M = \log_2 \left( 1 + \frac{P}{r_M^2 W_M} \right) = 3.46 \) bits per complex dimension. Furthermore, as the eavesdropper density \( \lambda_E \) increases, the probability mass of \( C_s \) becomes more concentrated around zero, in the sense that smaller realizations of \( C_s \) become more likely. Similarly, the impulses of the p.d.f. at the origin, given by \( F_{C_s}(0) \delta(c) \) (not represented in Fig. 4), also become larger as \( \lambda_E \) increases.

Figure 5 quantifies the secrecy outage probability \( p_{\text{outage}} \) in (16) versus the eavesdropper density \( \lambda_E \), for various values of \( P/W \). We observe that as \( \lambda_E \) increases, an outage in secrecy capacity of the main link becomes more likely, since there are more eavesdroppers that can exchange and combine the information, thus improving their ability to decode the secret message. Furthermore, we observe that as \( P/W \to \infty \), \( p_{\text{outage}} \) decreases monotonically, converging to the curve \( p_{\text{outage}} = \text{erf} \left( \frac{\pi \lambda E C_1/(b + 1)}{1 + r_M^2 W} \right) C_1/(b + 1) \).

VII. Conclusion

We established the fundamental security limits when the eavesdroppers are allowed to collude, by showing that this scenario is equivalent to a SIMO Gaussian wiretap channel. We derived the secrecy capacity of a legitimate link, considering that the positions of the illegitimate receivers follow an arbitrary spatial process \( \Pi_{E} \). Then, for the case where \( \Pi_{E} \) is a spatial Poisson process, we characterized the distribution of the secrecy capacity, as well as the corresponding probabilities of existence and outage. Perhaps the most interesting insight to be gained from our results is the exact quantification of the impact of the eavesdropper density \( \lambda_E \) on the achievable secrecy rates — even a modest number of scattered attackers.
can dramatically reduce the levels of security that can be provided at the physical layer of a wireless communication network.

REFERENCES