In-Band Sensing of the Adversary's Channel for Secure Communication in Wireless Channels

Mehrdad Tahmasbi and Matthieu Bloch
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta GA 30332
Email: {mtahmasbi3, matthieu}@gatech.edu

Aylin Yener
Electrical Engineering Department
The Pennsylvania State University
University Park, PA 16802
Email: yener@engr.psu.edu

***Abstract*—We propose a model of secure communication over wireless channels in which the legitimate parties leverage Radio Tomographic Imaging (RTI) to learn the adversary. Specifically, we model the results of RTI as an "in band" sensing channel that provides causal information about the eavesdropper's path-loss to the transmitter. This ability to learn the path-loss is exploited to achieve secrecy, even in presence of an eavesdropper that moves to optimize its path-loss and improves its eavesdropping. We show that the secrecy rates achieved are the same as those that would have been obtained with hindsight, had the transmitter known the average path-loss ahead of time.**

I. Introduction

While cryptographic encryption solutions based on public and private keys have been widely and successfully used, even strong encryption protocols, such as the widely used WPA2, are not immune to flaws in their implementations. Wireless Physical-Layer Security [1]–[3] has the potential to address these challenges by providing security guarantees on which to fall back even if everything else fails. Despite much progress and success in the analysis of various adversarial models [4]–[8] and in the design of coding schemes [9], [10], the scope of Wireless Physical-Layer Security (WPLS) has been limited. This is in large part due to the fact that the formulations have either been under idealistic assumptions, in particular in regards to what is known to the legitimate parties about the adversary, e.g., its channel [11], or in overly pessimistic scenarios, in which nothing is known about the adversary's conditions [12] or that the adversary has control over the physical channel and can alter the system of the legitimate parties [5], [13].

We recently suggested that there might exist a realistic middle ground between these two extremes [14]. Specifically, we have proposed a variation of attacker-controlled state-dependent wiretap models, in which the transmitter also has the opportunity to causally "learn" the states chosen by the adversary. For Discrete Memoryless Channels (DMCs) and binary states, we showed the perhaps surprising result that the legitimate parties can achieve the rates that they would have obtained had they known *with hindsight* the fraction of channel used corresponding to each state used by the adversary. Although, this result suggests the possibility of jointly transmitting secret information and learning the adversary, the modeling was fairly abstract. The objective of the present work is to show how the framework put forward in [14] may be adapted to the scenario of [12], which is more directly relevant to WPLS. In particular, our main conceptual contribution is the idea that *the wireless medium enables the legitimate parties to learn the environment (and thus, the adversary) at the physical layer*, supported by experimental results that have exploited wireless communication devices for "device-free" localization and tomography, also known as Radio Tomographic Imaging (RTI) [15]. Our technical contribution is to extend the approach and results of [14] to the continuous case model of [12], which requires different technical tools.

The paper is organized as follows. In Section II, we motivate a model for WPLS with "in band sensing" of the adversary's channel that captures the ability to learn the adversary. In Section III, we develop our main result for this model, which states that the secrecy rates are those that would have been obtained with hindsight, had the transmitter known the average channel gain of the adversary ahead of time.

II. Wireless Model

We consider the situation in which a legitimate transmitter (Alice) attempts to communicate a secret message to a legitimate receiver (Bob) in the presence of an adversary (Eve). As in [12], Eve is assumed to be capable of strategically controlling her observations through the arbitrary choice of her fading gains. We assume that the channels are memoryless and that fading is dominated by path-loss. At every discrete time instant i, a symbol $x_i \in \mathbb{R}$ sent by Alice is received by Bob and Eve as $y_i \in \mathbb{R}$ and $z_i \in \mathbb{R}$, respectively, given by $y_i = hx_i + n_{m,i}$ and $z_i = g_i x_i + n_{e,i}$, where h and $\{g_i\}$ are positive real-valued path-loss coefficients, and $\{n_{m,i}\}$, $\{n_{e,i}\}$ are independent and identically distributed (i.i.d.) zero-mean Gaussian noises with variance one. We assume that the legitimate parties know the path-loss coefficient h between Alice and Bob, e.g., through the use of pilot symbols, and that h remains fixed for the duration of the transmission, which is relevant for situations with little mobility. However, in contrast with traditional models for WPLS, we only assume that $g_i \in \mathcal{G} \triangleq]0, g^*]$ for some known g^*; in particular, i) there

This work was supported in part by the NSF award 1527074.

is no known prior placed on g_i; ii) g_i could even change from one channel use to the next if the eavesdropper is moving to optimize its eavesdropping capability [4], [12]. In this setting, traditional notions of secrecy capacity or even outage secrecy capacity do not apply in that we do not have a prior setting of the communication length.

We assume, however, that Alice and Bob can enroll other wireless devices, such as those part of an Internet of Things (IoT) platform, to perform Radio Tomographic Imaging (RTI). Recent advances [15], [16] have shown that simple measurements, such as Receive Signal Strength (RSS), can provide sub-meter localization in challenging environments, even with passive objects. The localization information provided by RTI can then be transformed into path-loss information. We model the overall ability to perform RTI by the existence of a sensing channel providing information about $\{g_i\}$ to Alice and characterized at each time instant i by $\overline{x}_i = g_i x_i + \overline{n}_{e,i}$, where $\{\overline{n}_{e,i}\}$ is an i.i.d. zero-mean Gaussian noise with unit variance. This modeling abstracts the fine details of RTI, but nevertheless maintains the idea that information about g_i is obtained "in-band," through the same wireless channel as the transmission. This also captures the requirement that Alice should *participate* in RTI, and should potentially expend channel uses to obtain the information. We refer to this model as *in-band sensing of the adversary's channel.*

Formally, a code for this channel model is similar to [14]. Since the number of message bits is unknown at the beginning of transmission, we assume instead that Alice has K uniformly distributed bits $\mathbf{W} \triangleq (W_1, \cdots, W_K) \in \{0,1\}^K \triangleq \mathcal{M}$, and that only the first ψ bits will be transmitted. The encoder consists of N possibly stochastic functions $\mathbf{f} = (f_1, \cdots, f_N)$ where $f_i : \mathbb{R}^{i-1} \times \mathcal{M} \to \mathbb{R}$ outputs a symbol for the transmission over the channel based on the past observations of the sensing channel. The total number of transmitted bits $\psi : \mathbb{R}^N \to [\![0, K]\!]$ is a function of Alice's observations and is determined *after* the Nth transmission. The decoder is a function $\phi : \mathbb{R}^N \to \mathcal{M}$, which allows the receiver to form an estimate $(\widehat{W}_1, \cdots, \widehat{W}_K) = \phi(\mathbf{Y})$ of the transmitted bits. Since the channel is varying according to Eve's path-loss coefficients, Bob is *not* required to reliably decode all bits; instead, we assume that there exists a function $\widehat{\psi} : \mathbb{R}^N \to [\![0, K]\!]$ that estimates the number of bits actually transmitted. The quadruple $(\mathbf{f}, \phi, \psi, \widehat{\psi})$ defines an (N, K) code $\mathcal{C}$, and the functions $\mathbf{f}$, ϕ, ψ, and $\widehat{\psi}$ are assumed to be publicly known. For all sequences of N path-loss coefficients $\mathbf{g}$, the reliability is measured with a probability of error defined as

$$P_e(\mathcal{C}|\mathbf{g}) \triangleq \mathbb{P}\Big(\widehat{\psi}(\mathbf{Y}) \neq \psi(\overline{\mathbf{X}}) \text{ or } \exists k \in [\![1, \widehat{\psi}(\mathbf{Y})]\!] : \widehat{W}_k \neq W_k | \mathbf{g}\Big), \quad (1)$$

and secrecy is measured through the mutual information $\mathbb{I}(\mathbf{W}; \mathbf{Z}|\mathbf{g})$. The rate of the code is a function of the adversary's path-loss coefficients and is a random variable defined as $\frac{\psi(\overline{\mathbf{X}})}{n}$. The average power of the code is also defined as $\frac{1}{N}\sum_{i=1}^{N} \mathbb{E}\big(X_i^2\big)$.

Definition 1: For a fixed sequence $\{\mathbf{g}_N \in \mathcal{G}^N\}_{N \geqslant 1}$ of path-loss coefficients, we say that a sequence of (N, K_N) codes $\{\mathcal{C}_N = (\mathbf{f}_N, \phi_N, \psi_N, \widehat{\psi}_N)\}_{N \geqslant 1}$ achieves a rate R with average power P, if and only if, we have

$$\lim_{N\to\infty} \frac{1}{N}\sum_{i=1}^{N} \mathbb{E}\big(X_i^2\big) \leqslant P, \quad \lim_{N\to\infty} \mathbb{I}(\mathbf{W}; \mathbf{Z}|\mathbf{g}_N) = 0, \quad (2)$$

$$\lim_{N\to\infty} P_e(\mathcal{C}_N|\mathbf{g}_N) = 0, \text{ and } \lim_{N\to\infty} \mathbb{P}\left(\frac{\psi(\overline{\mathbf{X}})}{N} \leqslant R\right) = 0. \quad (3)$$

III. Main Result

Our main result is the characterization of the secrecy rates that can be achieved in the proposed model for *any* sequence of path loss for the adversary.

Theorem 1: For $\zeta > 0$, there exists a sequence of (N, K_N) codes $\{\mathcal{C}_N\}_{N \geqslant 1}$ that, for all I_Z, achieves the secrecy rate

$$\left[\frac{1}{2}\log(1 + h^2 P) - I_Z\right]^+ - \zeta \quad (4)$$

for every sequence $\{\mathbf{g}_N\}_{N \geqslant 1}$ such that

$$\lim_{N\to\infty} \frac{\sum_{i=1}^{N} \frac{1}{2}\log(1 + g_i^2 P)}{N} = I_Z. \quad (5)$$

Theorem 1 is meaningful in that i) it claims the existence of a *universal* sequence of codes that achieves secrecy for all path-loss sequences; ii) the secrecy rate is what would be achieved had we known the average path-loss ahead of time. In other words, although learning is strictly causal and the path-loss of the adversary is not predicted, our proposed scheme performs as if the path-loss of the adversary had been known in advance. We also emphasize that, as evident from our proof of Theorem 1, the protocol operates in the regime of finite blocklength without requiring any properties on the path-loss sequence of the adversary. The asymptotic condition in (5) is merely for convenience and elegance of the theorem statement.

IV. Proof of Theorem 1

The proof follows the steps of [12], with the necessary modifications to account for layered secrecy coding and the presence of causal sensing. We start by recalling a concentration of measure result that will prove useful in our analysis.

Theorem 2 (Hanson-Wright): Let $\mathbf{X} = (X_1, \cdots, X_n)^T$ be a random vector such that $X_1, \cdots, X_n$ are independent, and for all $i \in [\![1, n]\!]$, we have $\mathbb{E}(X_i) = 0$ and

$$\|X_i\|_{\psi_2} \triangleq \sup_{p \geqslant 1} p^{-\frac{1}{2}} \left(\mathbb{E}(|X_i|^p)\right)^{\frac{1}{p}} \leqslant K. \quad (6)$$

Then, there exists a universal constant $c > 0$ such that for any $n \times n$ matrix and any $t > 0$, we have

$$\mathbb{P}\big(|\mathbf{X}^T A \mathbf{X} - \mathbb{E}\big(\mathbf{X}^T A \mathbf{X}\big)| \geqslant t\big) \leqslant 2\exp\left[-c\min\left(\frac{t^2}{K^4\|A\|_{\text{HS}}^2}, \frac{t}{K^2\|A\|}\right)\right], \quad (7)$$

where

$$\|A\| \triangleq \sup_{\mathbf{x}\in\mathbb{R}^n:\|\mathbf{x}\|_2=1} \|A\mathbf{x}\|_2 \text{ and } \|A\|_{\text{HS}} \triangleq \sqrt{\text{tr}\left(A^T A\right)}. \quad (8)$$

Lemma 1: Let $X_1, \cdots, X_n, N_1, \cdots, N_n$ be a sequence of independent random variables such that for all $i \in [\![1, n]\!]$, X_i and N_i are distributed according to $\mathcal{N}(0, P)$ and $\mathcal{N}(0, 1)$, respectively. Let us define $Z_i \triangleq g_i X_i + N_i$ for constants $g_1, \cdots, g_n \in \mathbb{R}$. We then have

$$\mathbb{P}\left(\sum_{i=1}^n \log \frac{p_{Z_i|X_i}(Z_i|X_i)}{p_{Z_i}(Z_i)} \geqslant \frac{1}{2}\sum_{i=1}^n \log\left(1+g_i^2 P\right) + n\zeta\right) \leqslant 2\exp\left(-n\xi\right), \quad (9)$$

where $p_{Z_i|X_i}$ is the conditional Probability Distribution Function (PDF) of Z_i given X_i, p_{Z_i} is the PDF of Z_i, and

$$\xi \leqslant \frac{c\zeta}{K^2} \min_i \min\left(\frac{\zeta}{K^2\left(g_i^4(P^2+1)+2g_i^2\right)}, \frac{2}{\left|g_i\sqrt{g_i^2(1+P)^2+4}\right|}\right) \quad (10)$$

with $K \triangleq \sqrt{2/\pi}\max(\sqrt{P}, 1)$. In particular, if $|g_i| \leqslant g^*$ for all $i \in [\![1, n]\!]$, ξ can be chosen such that it depends only on c, ζ, P, and g^*.

Proof: Since Z_i is distributed according to $\mathcal{N}(0, 1+g_i^2 P)$, and given $X_i = x_i$, Z_i is distributed according to $\mathcal{N}(g_i x_i, 1)$, by definition, we have

$$\begin{aligned}
&\log \frac{p_{Z_i|X_i}(Z_i|Z_i)}{p_{Z_i}(Z_i)} \\
&= \frac{1}{2}\log\left(1+g_i^2 P\right) - \frac{(Z_i - g_i X_i)^2}{2} + \frac{Z_i^2}{2(1+g_i^2 P)} \quad (11)\\
&= \frac{1}{2}\log\left(1+g_i^2 P\right) - \frac{g_i^2 P N_i^2}{2(1+g_i^2 P)} + \frac{g_i^2 X_i^2}{2(1+g_i^2 P)} \\
&\qquad + \frac{g_i X_i N_i}{1+g_i^2 P}. \quad (12)
\end{aligned}$$

For $\mathbf{X} \triangleq (N_1, \cdots, N_n, X_1, \cdots, X_n)^T \in \mathbb{R}^{2n}$ and

$$A = \frac{1}{2}\begin{bmatrix} \text{Diag}\left(-\frac{g_1^2 P}{1+g_1^2 P}, \cdots, -\frac{g_n^2 P}{1+g_n^2 P}\right) & \text{Diag}\left(\frac{g_1}{1+g_1^2 P}, \cdots, \frac{g_n}{1+g_n^2 P}\right) \\ \text{Diag}\left(\frac{g_1}{1+g_1^2 P}, \cdots, \frac{g_n}{1+g_n^2 P}\right) & \text{Diag}\left(\frac{g_1^2}{1+g_1^2 P}, \cdots, \frac{g_n^2}{1+g_n^2 P}\right) \end{bmatrix}, \quad (13)$$

we therefore obtain that

$$\begin{aligned}
&\mathbb{P}\left(\sum_{i=1}^n \log \frac{p_{Z_i|X_i}(Z_i|X_i)}{p_{Z_i}(Z_i)} \geqslant \frac{1}{2}\sum_{i=1}^n \log(1+g_i^2 P) + n\zeta\right) \\
&= \mathbb{P}\left(\mathbf{X}^T A\mathbf{X} - \mathbb{E}\left(\mathbf{X}^T A\mathbf{X}\right) \geqslant \zeta n\right). \quad (14)
\end{aligned}$$

To apply Theorem 2 to the right hand side of the above equality, note that

$$\|N_i\|_{\psi_2} = \sup_{p\geqslant 1} p^{-\frac{1}{2}}\left(\mathbb{E}(|N_i|^p)\right)^{\frac{1}{p}} \quad (15)$$

$$= \sup_{p\geqslant 1} p^{-\frac{1}{2}}\left(\frac{(2)^{\frac{p}{2}}\Gamma\left(\frac{p+1}{2}\right)}{\sqrt{\pi}}\right)^{\frac{1}{p}} = \sqrt{\frac{2}{\pi}}, \quad (16)$$

and similarly,

$$\|X_i\|_{\psi_2} = \sqrt{\frac{2P}{\pi}}. \quad (17)$$

In addition, one can check that

$$\|A\| \leqslant \frac{1}{2}\max_{i\in[\![1,n]\!]}\left|g_i\sqrt{g_i^2(1+P)^2+4}\right|, \quad (18)$$

and

$$\|A\|_{\text{HS}} \leqslant \sqrt{n}\max_{i\in[\![1,n]\!]}\sqrt{g_i^4(P^2+1)+2g_i^2}. \quad (19)$$

We therefore obtain for $K \triangleq \sqrt{2/\pi}\max(\sqrt{P}, 1)$ that

$$\begin{aligned}
&\mathbb{P}\left(\mathbf{X}^T A\mathbf{X} - \mathbb{E}\left(\mathbf{X}^T A\mathbf{X}\right) \geqslant \zeta n\right) \\
&\leqslant 2\exp\left[-c\min\left(\frac{\zeta^2 n^2}{K^4\|A\|_{\text{HS}}^2}, \frac{\zeta n}{K^2\|A\|}\right)\right], \quad (20)
\end{aligned}$$

which is less than $2\exp(-\xi n)$ for

$$\xi = \frac{c\zeta}{K^2}\min_i \min\left(\frac{\zeta}{K^2\left(g_i^4(P^2+1)+2g_i^2\right)}, \frac{2}{\left|g_i\sqrt{g_i^2(1+P)^2+4}\right|}\right). \quad (21)$$

If $|g_i| \leqslant g^*$ for all $i \in [\![1, n]\!]$, we also lower-bound ξ by

$$\frac{c\zeta}{K^2}\min\left(\frac{\zeta}{K^2\left(g^{*4}(P^2+1)+2g^{*2}\right)}, \frac{2}{g^*\sqrt{g^{*2}(1+P)^2+4}}\right), \quad (22)$$

which depends only on c, ζ, P, and g^*. ■

We now show the existence of an encoder guaranteeing layered-secrecy for all fading coefficients of Eve. Specifically, let $\mathbb{I}_Z(g) \triangleq \frac{1}{2}\log(1+g^2 P)$ and consider a random encoder $F : \{0,1\}^k \to \mathbb{R}^n$ encoding k uniformly distributed bits $\mathbf{W} = (W_1, \cdots, W_k)$ into a codeword of length n, $\mathbf{X}$. We then prove that for an appropriate distribution on the random encoder, with high probability, for all sequences of fading coefficients $\mathbf{g} \in \mathcal{G}^n$, if the sequence $\mathbf{X}$ is transmitted over an Additive White Gaussian Noise (AWGN) channel described with fading coefficients $\mathbf{g}$ to obtain sequence $\mathbf{Z} \in \mathbb{R}^n$, the mutual information between the first $\approx k - \sum_{i=1}^n \mathbb{I}_Z(g_i)$ bits of $\mathbf{W}$ and $\mathbf{Z}$ is negligible, as formalized in the next lemma.

Lemma 2: Let $\zeta > 0$, k and $m(\mathbf{g}) \triangleq k - \sum_{i=1}^n \mathbb{I}_Z(g_i) - \zeta n$ for all $\mathbf{g} \in \mathcal{G}^n$. Let $F : \{0,1\}^k \to \mathbb{R}^n$ be a random encoder whose codewords are drawn independently according

to $\mathcal{N}(0,P)^{\otimes n}$. There exists $\xi > 0$ depending only on c, ζ, P, and g^*

$$\mathbb{P}_F(\forall \mathbf{g} \in \mathcal{G}^n \text{ s.t. } m(\mathbf{g}) \geqslant \zeta n, \\ \mathbb{I}\big(W_1, \cdots, W_{m(\mathbf{g})-\zeta n}; \mathbf{Z}|\mathbf{g}\big) \leqslant 2^{-\xi n}) \geqslant 1 - 2^{-2^{\xi n}}. \quad (23)$$

Proof: We prove the lemma in four steps as in [12].

a) Step 1: **We show that for a fixed g, the expectation under random coding of the information leakage measured in terms of *the variational distance* is exponentially small.** Let $\widehat{P}_{\mathbf{WZ}}$ be the induced probability measure on $\mathbf{W}$ and $\mathbf{Z}$ when using the encoder F.[1] Let $X_1, \cdots, X_n$ and $N_1, \cdots, N_n$ be two i.i.d. sequences with generic distributions $\mathcal{N}(0,P)$ and $\mathcal{N}(0,1)$, respectively. Let $Z_i \triangleq g_i X_i + N_i$ for $i \in [\![1,n]\!]$. By deriving secrecy from resolvability, we obtain

$$\mathbb{E}_F\Big(\mathbb{V}\Big(\widehat{P}_{W_1\cdots W_{m(\mathbf{g})}\mathbf{Z}}, \widehat{P}_{W_1\cdots W_{m(\mathbf{g})}} \times \widehat{P}_{\mathbf{Z}}\Big)\Big) \\ \leqslant 2\mathbb{E}_F\Big(\mathbb{V}\Big(\widehat{P}_{W_1\cdots W_{m(\mathbf{g})}\mathbf{Z}}, \widehat{P}_{W_1\cdots W_{m(\mathbf{g})}} \times P_{\mathbf{Z}}\Big)\Big) \quad (24)$$

$$= 2 \sum_{w_1,\cdots,w_{m(\mathbf{g})}} \frac{1}{2^{m(\mathbf{g})}} \mathbb{E}_F\Big(\mathbb{V}\Big(\widehat{P}_{\mathbf{Z}|W_1=w_1\cdots W_m=w_{m(\mathbf{g})}}, P_{\mathbf{Z}}\Big)\Big) \quad (25)$$

$$\overset{(a)}{\leqslant} 2\mathbb{P}\left(\sum_{i=1}^n \log \frac{p_{Z_i|X_i}(Z_i|X_i)}{p_{Z_i}(Z_i)} \geqslant \gamma\right) + 2^{\frac{\gamma-(k-m(\mathbf{g}))}{2}+1} \quad (26)$$

where $P_{\mathbf{Z}}$ is the distribution of random vector $\mathbf{Z} = (Z_1, \cdots, Z_n)$, and (a) follows from [17, Lemma 2] for all $\gamma \in \mathbb{R}$. Choosing

$$\gamma = \sum_{i=1}^n \mathbb{I}_Z(g_i) + \frac{\zeta n}{2}, \quad (27)$$

Lemma 1 implies that for some ξ_1' depending on c, P, ζ, g^*,

$$\mathbb{P}\left(\sum_{i=1}^n \log \frac{p_{Z_i|X_i}(Z_i|X_i)}{p_{Z_i}(Z_i)} \geqslant \gamma\right) \leqslant 2^{-\xi_1' n}, \quad (28)$$

and by the definition of $m(\mathbf{g})$ and γ, we have

$$2^{\frac{\gamma-(k-m(\mathbf{g}))}{2}+1} \leqslant 2^{-\frac{\zeta n}{4}+1}. \quad (29)$$

Thus, if $\xi_1 < \min(\xi_1', \zeta/4)$ for large enough n we have

$$\mathbb{E}_F\Big(\mathbb{V}\Big(\widehat{P}_{W_1\cdots W_{m(\mathbf{g})}\mathbf{Z}}, \widehat{P}_{W_1\cdots W_{m(\mathbf{g})}} \times \widehat{P}_{\mathbf{Z}}\Big)\Big) \leqslant 2^{-\xi_1 n}. \quad (30)$$

b) Step 2: **We show that, with high probability, the information leakage measured in variational distance is exponentially small for a fixed fading coefficients $\mathbf{g} \in \mathcal{G}^n$ such that $m(\mathbf{g}) \geqslant \zeta n$.** One can show that

$$\mathbb{P}_F\Big(\mathbb{V}\Big(\widehat{P}_{W_1\cdots W_{m(\mathbf{g})}\mathbf{Z}}, \widehat{P}_{W_1\cdots W_{m(\mathbf{g})}} \times P_{\mathbf{Z}}\Big) \geqslant 2^{-\xi_1 n+1}\Big) \\ \leqslant \exp\Big(-2^{m(\mathbf{g})-2\xi_1 n+1)}\Big). \quad (31)$$

[1]Note that $\mathbf{W}$ and $\mathbf{Z}$ are discrete and continuous random variables, respectively, and therefore, their joint probability measure is a mixed of continuous and discrete probability measures.

By our choice of $\mathbf{g}$ and ξ_1 have

$$m(\mathbf{g}) - 2\xi_1 n + 1 \geqslant \frac{1}{2}\zeta n. \quad (32)$$

We therefore obtain for $\xi_2 < \min(\xi_1, \zeta/2)$

$$\mathbb{P}_F\Big(\mathbb{V}\Big(\widehat{P}_{W_1\cdots W_{m(\mathbf{g})}\mathbf{Z}}, \widehat{P}_{W_1\cdots W_{m(\mathbf{g})}} \times P_{\mathbf{Z}}\Big) \geqslant 2^{-\xi_2 n}\Big) \leqslant 2^{-2^{\xi_2 n}}. \quad (33)$$

c) Step 3: **We show how an upper-bound on the information leakage with variational distance implies an upper-bound on the information leakage with relative entropy.** One can show that

$$\mathbb{I}\big(W_1, \cdots, W_{m(\mathbf{g})}; \mathbf{Z}\big) \\ \leqslant 4m(\mathbf{g})\mathbb{V}\Big(\widehat{P}_{W_1\cdots W_{m(\mathbf{g})}\mathbf{Z}}, \widehat{P}_{W_1\cdots W_{m(\mathbf{g})}} \times P_{\mathbf{Z}}\Big), \quad (34)$$

where (a) follows from [18, Eq. (360)]. As a result, we have for $0 < \xi_3 < \min(\xi_2)$ and n large enough

$$\mathbb{P}\big(\mathbb{I}\big(W_1, \cdots, W_{m(\mathbf{g})}; \mathbf{Z}\big) \geqslant 2^{-\xi_3 n}\big) \leqslant 2^{-2^{\xi_3 n}}. \quad (35)$$

d) Step 4: **With proper quantization, we show how to guarantee secrecy for all $\mathbf{g} \in \mathcal{G}^n$.** For any $\Delta > 0$, we define $Q_\Delta(g) \triangleq \Delta\lceil g/\Delta \rceil$ and $Q_\Delta^n(\mathbf{g}) = (Q_\Delta(g_1), \cdots, Q_\Delta(g_n))$, for which one can check that $|Q_\Delta(g) - g| \leqslant \Delta$. Since $\mathbb{I}_Z(g)$ is uniformly continuous on $\mathcal{G}$, there exists positive integer d depending on ζ, g^*, and P such that for all $g_1, g_2 \in \mathcal{G}$, $|g_1 - g_2| \leqslant g^*/d$ implies that $|\mathbb{I}_Z(g_1) - \mathbb{I}_Z(g_2)| < \zeta$. By setting $\Delta = g^*/d$, we therefore have

$$m(Q_\Delta^n(\mathbf{g})) = k - \sum_{i=1}^n \mathbb{I}_Z(Q_\Delta(g_i)) - \zeta n \quad (36)$$

$$\geqslant k - \sum_{i=1}^n (\mathbb{I}_Z(g_i) + \zeta) - \zeta n \quad (37)$$

$$= m(\mathbf{g}) - \zeta n \quad (38)$$

Note that for any $0 < g_1 \leqslant g_2$ the channel $Z = g_1 X + N$ is degraded with respect to the channel $Z = g_2 X + N$. Hence, for a fixed encoder f, by the data processing inequality, we have for all $m \in [\![0,n]\!]$

$$\mathbb{I}(W_1, \cdots, W_m; \mathbf{Z}|\mathbf{g}) \leqslant \mathbb{I}(W_1, \cdots, W_m; \mathbf{Z}|Q_\Delta^n(\mathbf{g})). \quad (39)$$

and using a union bound one can show

$$\mathbb{P}_F(\forall \mathbf{g} \in \mathcal{G}^n \text{ s.t. } m(\mathbf{g}) \geqslant \zeta n, \\ \mathbb{I}\big(W_1, \cdots, W_{m(\mathbf{g})-\zeta n}; \mathbf{Z}|\mathbf{g}\big) \leqslant 2^{-\xi n}) \geqslant 1 - 2^{-2^{\xi n}}. \quad (40)$$

■

Corollary 1: For all $\zeta > 0$ and $P > 0$, there exists $\xi > 0$ such that for n large enough and $k \triangleq n\left(\frac{1}{2}\log\left(1 + h^2 P\right) - \zeta\right)$, there exists a pair of encoder/decoder (f, ϕ) where $f : \{0,1\}^k \to \mathbb{R}^n$ and $\phi : \mathbb{R}^n \to \{0,1\}^k$ with probability of error less than $2^{-n\xi}$ and for all $\mathbf{g} \in \mathcal{G}^n$ such that $m(\mathbf{g}) \geqslant \zeta n$, we have

$$\mathbb{I}\big(W_1, \cdots, W_{\max(0,m(\mathbf{g}))}; \mathbf{Z}|\mathbf{g}\big) \leqslant 2^{-\xi n}. \quad (41)$$

Finally the average power of the code is less than $P+o(1)$. [2]

V. Our Proposed Coding Scheme

Fixing $n, B, t, t' \in \mathbb{N}$, the transmission happens over $N = B(n+t)+t'$ channel uses with B sub-blocks of length $n+t$.

a) Encoding: Let $\mathbf{W}^b = (W_1^b, \cdots, W_k^B)$ be the message bits to be transmitted in sub-block b and $\mathbf{L}^b = (L_1^b, \cdots, L_k^B)$ be auxiliary uniformly distributed bits used for encoding of sub-block b. We also define $\mathbf{A}^0 \triangleq (0, \cdots, 0) \in \{0,1\}^k$ and $m^0 \triangleq 0$. At the beginning of sub-block $b \in [\![1, B]\!]$, Alice forms the sequence $\mathbf{A}^b = (A_1^b, \cdots, A_k^b)$ according to

$$A_i^b \triangleq \begin{cases} A_i^{b-1} \oplus W_i^b & i \in [\![1, m^{b-1}]\!], \\ L_i^b & i \in [\![m^{b-1}, k]\!]. \end{cases} \tag{42}$$

Alice then encodes $\mathbf{A}^b$ into the codeword of length n $\mathbf{X}^b \triangleq f(\mathbf{A}^b)$ using the encoder f as in Corollary 1. Alice also chooses t positions $\mathbf{J}^b = (J_1, \cdots, J_t)$ uniformly at random with $1 \leqslant J_1 < \cdots < J_t \leqslant n+t$ for estimation. She subsequently transmits η, whose value will be specified later, on the positions in $\mathbf{J}^b$ and transmits $\mathbf{X}^b$ on the remaining n positions. At the end of sub-block b, Alice sets

$$m^b \triangleq k - \frac{n}{t} \sum_{i=1}^{t} \mathbb{I}_Z \left(\frac{\overline{X}_{J_i}}{\eta} \right) - 2\zeta n. \tag{43}$$

Alice finally uses the last t' channel uses to send $\mathbf{J}^1, \cdots, \mathbf{J}^B$ together with $m^1, \cdots, m^B$ using any channel code.

b) Decoding: Bob first decodes $\mathbf{J}^1, \cdots, \mathbf{J}^B$ and $\mathbf{m}^1, \cdots, \mathbf{m}^B$ and forms the sequence $\mathbf{Y}^1, \cdots, \mathbf{Y}^B$ where $\mathbf{Y}^b$ is his observation in sub-block b on the positions Alice did not used for estimation. He then decodes $\mathbf{A}^b$ as $\widehat{\mathbf{A}}^b \triangleq \phi(\mathbf{Y}^b)$ for $b \in [\![1, B]\!]$ and defines

$$\widehat{W}_i^b = \widehat{A}_i^b \oplus \widehat{A}_{i-1}^b \quad i \in [\![1, m^{b-1}]\!]. \tag{44}$$

c) Reliability Analysis: Since the probability of error in each sub-block is $2^{-n\xi}$, the overall one is bounded by $B2^{-n\xi}$.

d) Secrecy Analysis: In the following lemma, we first show that m^b is a good approximation of $m(\mathbf{g}^b)$.

Lemma 3: For a constant $\zeta' > 0$ depending on ζ and g^*,

$$\mathbb{P}\big(m(\mathbf{g}^b) - 2\zeta n \leqslant m^b \leqslant m(\mathbf{g}^b)\big) \geqslant 1 - 2ne^{-\frac{\eta^2\zeta'^2}{2}} - 2e^{-\frac{t\zeta^2}{2\mathbb{I}_Z(g^*)^2}}. \tag{45}$$

Proof: Omitted because of space limit. ■

Following the same calculation for DMCs [14], we obtain that

$$\mathbb{I}(\mathbf{Z}; \mathbf{W}|\mathbf{g}) \leqslant KB \left(2ne^{-\frac{\eta^2\zeta'^2}{2}} + 2e^{-\frac{t\zeta^2}{2\mathbb{I}_Z(g^*)^2}} \right) + B^2 2^{-\xi n}.$$

[2] As ζn appears in $m(\mathbf{g})$, by properly re-defining ζ and ξ, we can remove the condition $m(\mathbf{g}) \geqslant \zeta n$ and guarantee the secrecy of the first $m(\mathbf{g})$ bits.

e) Rate Analysis: By Lemma 3, the achievable rate is

$$\frac{1}{N} \sum_{b=1}^{B-1} m^b \geqslant \left[\frac{1}{2} \log(1+Ph^2) - \frac{1}{N} \sum_{b=1}^{B} \sum_{i=1}^{n} \mathbb{I}_Z(g_i^b) + O(\zeta + \frac{1}{B}) \right]^+.$$

with probability at least $1 - B(2ne^{-\frac{\eta^2\zeta'^2}{2}} + 2e^{-\frac{t\zeta^2}{2\mathbb{I}_Z(g^*)^2}})$.

f) Power Analysis: On the positions used for data transmission the average power is less than $P+o(1)$ by Corollary 1. On the positions used for estimation, the average power is η. The overall average power would be $\frac{t}{n'}\eta + \frac{n}{n'}(P+o(1))$. Therefore, to achieve the rate R with average power P, it is enough to choose $n' = \lfloor \sqrt{N} \rfloor$, $t = \lfloor \sqrt{n'} \rfloor$, and $\eta = \sqrt{t}$.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, October 2011.

[2] Y. Liang, H. V. Poor, and S. S. (Shitz), *Information-Theoretic Security*, ser. Foundations and Trends in Communications and Information Theory. Delft, Netherlands: Now Publishers, 2009, vol. 5, no. 1–5.

[3] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct 2015.

[4] X. He and A. Yener, "Secrecy when the eavesdropper controls its channel states," in *Proc. of IEEE International Symposium on Information Theory*, St. Petersburg, Russia, August 2011, pp. 618–622.

[5] M. Wiese, J. Nötzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack —correlated random coding capacities under strong secrecy criteria," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3844–3862, Jul. 2016.

[6] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Arbitrarily varying wiretap channels with type constrained states," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7216–7244, Dec. 2016.

[7] M. Nafea and A. Yener, "Wiretap channel II with a noisy main channel," in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015, pp. 1159–1163.

[8] ——, "A new wiretap channel model and its strong secrecy capacity," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 2077–2092, March 2018.

[9] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Proc. of CRYPTO 2012*, vol. 7417, 2012, pp. 294–311.

[10] M. R. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of IEEE*, vol. 103, no. 10, pp. 1725–1746, October 2015.

[11] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[12] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6844–6869, 2014.

[13] P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 970–983, Feb. 2016.

[14] M. Tahmasbi, M. R. Bloch, and A. Yener, "Learning adversary's actions for secret communication," in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 2713–2717.

[15] N. Patwari and J. Wilson, "RF sensor networks for device-free localization: Measurements, models, and algorithms," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1961–1973, Nov 2010.

[16] Y. Zhao, N. Patwari, J. M. Phillips, and S. Venkatasubramanian, "Radio tomographic imaging and tracking of stationary and moving people via kernel distance," in *Proceedings of the 12th International Conference on Information Processing in Sensor Networks*, 2013, pp. 229–240.

[17] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channels," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, April 2006.

[18] I. Sason and S. Verdu, "f -divergence inequalities," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 5973–6006, Nov 2016.