Improving Physical-Layer Security through Random Beamforming

Darren Lund[‡], Marco A. C. Gomes[*], João P. Vilela[†], and Willie K. Harrison[‡]
[*]Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Portugal
[†]CISUC and Department of Informatics Engineering, University of Coimbra, Portugal
[‡]Department of Electrical and Computer Engineering, Brigham Young University, UT, USA
Emails: darrenlund@byu.edu, marco@co.it.pt, jpvilela@dei.uc.pt, willie.harrison@byu.edu

***Abstract*—In this paper, we study Phyical-Layer Security in a SISO transmission where the primary transmitter, Alice, has multiple antennas, and all receivers, Bob and Eve, have a single antenna. In this instance, we specifically look at the case where transmissions are packet based, so Bob and Eve each have a Packet Erasure Channel (PEC), and Alice utilizes random directional beamforming. In our physics based model, we show numerically that, of the options explored, the best choice is to transmit directly at the intended receiver, Bob, for all transmissions. We define best by utilizing two methods, secrecy capacity and secrecy probability.**

I. Introduction

Establishing secure communications is of paramount importance for modern society. In order to accomplish this, many systems and tools have been developed to increase security through cryptography and encoding, and increase reliability by decreasing the amount of noise in the transmission channel. Unfortunately, no channel is completely noiseless. However, a usually unused portion of the Open Systems Interconnection (OSI) Protocol stack, the physical layer, may be capable of utilizing this noise to further enhance security.

Most utilizations of beamforming for physical-layer security include either randomly generating beamforming weights, as in REFERENCE KRIKIDIS, or include adding noise for jamming, as in REFERENCE HUI-MING & ZHU, and usually require knowledge of the eavesdropper's channel. In this paper, we instead assume that we don't know the eavesdroppers location, and explore the possibility of using random directional beamforming in order to increase physical-layer security by utilizing a high probability of packet erasure in a Packet Erasure Wiretap Channel (PEWC) to ensure that Bob receives some packet that Eve doesn't. Random directional beamforming involves selecting a random variable $\Phi(\phi)$, defined on the interval $\left[-\frac{\phi}{2}, \frac{\phi}{2}\right]$ for some $\phi \in \mathbb{R}_{\geq 0}$, and transmits each packet in a direction determined by Φ. The intent of this scheme is to allow some packets to be transmitted such that the bit error of the main channel, ϵ_m, is greater than the bit error of the wiretap channel, ϵ_w, and ϵ_c for an arbitrary channel. This then allows a coding scheme like the ones described in [1], [2] to be employed, which will take advantage of this difference to ensure information security. The primary reason dropping a packet improves security is that in [1], [2], every packet is necessary for decoding, and while Bob can request retransmission of the packets erased by his channel, Eve cannot. Thus, if Eve misses so much as a single packet that Bob receives, she cannot decode the message. Random directional beamforming, coupled with a high probability of packet erasure inside the primary beam will be used to guarantee that at some point this happens. After a small number of these transmissions, Bob's advantage will already have been established, so normal transmitting techniques can be employed for the remaining packets without decreasing security.

This paper is meant as a proof of concept; namely to quantify how much security can be gained by beamforming to take advantage of a PEWC. As such, the set up used for the calculations and results will not be very sophisticated in terms of modern transmission techniques. It is hoped, rather, that the ideas provided will allow users to adapt their own systems to increase security at the physical layer. Throughout the paper, we assume a general wiretap channel model with feedback, shown in Fig. 1. While the calculations used for Fig. 3 allow for Eve to be closer to or further from Alice than Bob, all calculations after that were made as if Bob and Eve are equidistant from Alice, for simplicity. Simple changes can be made to account for variable distance, but those results are not included in this paper.

The rest of the paper is organized as follows. The set-up for the problem we are trying to solve, followed by an explanation of the work done to solve that problem, then the results of tested simulations, and finally, a conclusion.

II. Problem Set-Up

Ideally, the problem of transmitting is to ensure reliability to any intended receiver, and security against any eavesdropper. That is, if B_p is the probability that Bob receiving the transmitted message, and E_p is the probability that Eve receives that message, then at the end of the transmission, then $B_p = 1$ and $E_p = 0$. The piece of this problem that we address is to

This work was partially funded by the following entities and projects: the US National Science Foundation (Grant Award Number 1761280), the FLAD project INCISE (Interference and Coding for Secrecy), project SWING2 (PTDC/EEI-TEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização - COMPETE 2020 and by National Funds from FCT - Fundação para a Ciência e a Tecnologia, through projects POCI-01-0145-FEDER-016753 and UID/EEA/50008/2013.

calculate the average secrecy capacity, defined as the average across all transmissions of the main channel capacity minus the wiretap channel capacity, and the average secrecy probability, which is defined as the average probability that Bob received a packet and Eve dropped that same packet for any given transmission as a function of the angle θ for a given random variable Φ and associated input ϕ, as depicted in Fig 2. We do this by calculating the Packet Erasure Probability (PEP), denoted with the variable Ψ. This is because the equipment we assume to be in use, which is packet based, will receive a packet and either accept it as accurate, or reject it in it's entirety. Thus, for a single transmission from Alice with packets of length M, then the secrecy capacity is

$$\begin{aligned} C_s &= \left(\left(1 - \Psi\left(\Phi\left(\phi\right), 0\right)\right) - \left(1 - \Psi\left(\Phi\left(\phi\right), \theta\right)\right)\right) M \\ &= \left(\Psi\left(\Phi\left(\phi\right), \theta\right) - \Psi\left(\Phi\left(\phi\right), 0\right)\right) M \end{aligned}$$

and, since the probability that Bob receives the packet is independent of the probability that Eve receives the packet, the secrecy probability is

$$P_s = \left(1 - \Psi\left(\Phi\left(\phi\right), 0\right)\right) \Psi\left(\Phi\left(\phi\right), \theta\right)$$

While the overall goal would be to maximize these two values, we numerically calculate these values for different choices of Φ and ϕ as functions of θ. To allow this to drive our model, we shall assume that to encode the message, Alice will use a scheme like the one outlined by Adi Shamir in REFERENCE HOW TO SHARE A SECRET, that allows us to break a message into n encoded packets of length M in such a way that any k packets will ensure full message recovery while $k-1$ or fewer packages guarantee that the message cannot be fully recovered. We do not outline the specifics here, but the process develops what is called a (k, n) *threshold scheme*, which we will assume is being used for all transmissions. After dividing the message into these packets, we select k packets to transmit, so that reconstruction of the message fails if any antenna fails to receive a single packet. Thus reliability is achieved if Bob receives k distinct packets, and security is achieved if Eve receives no more than $k-1$ distinct packets, as desired. In order to transmit these packets, we will use the process of beamforming.

A. Beamforming

Beamforming is a means of using multiple antenna to increase signal power in a certain direction relative to either the transmitter or receiver. If done at the transmitter, as is in our model, this is achieved by phase shifting the signal from each antenna to generate constructive interference at the desired angle (in this case, $\theta = 0$), as shown in Fig. 2. For the entirety of this paper, we will assume that the receiver, Bob, and the eavesdropper, Eve, are in the far field from Alice; that is, they are far enough away that the signal from each of Alice's transmitters appear as a plane, instead of curved. Since each antenna is transmitting the same signal, the phase shift needed will correspond to a time delay in the transmission of each antenna. This can be represented by

$$y(t) = \sin\left(2\pi f(t + \delta t)\right) = \sin\left(2\pi f t + \alpha\right) \tag{1}$$

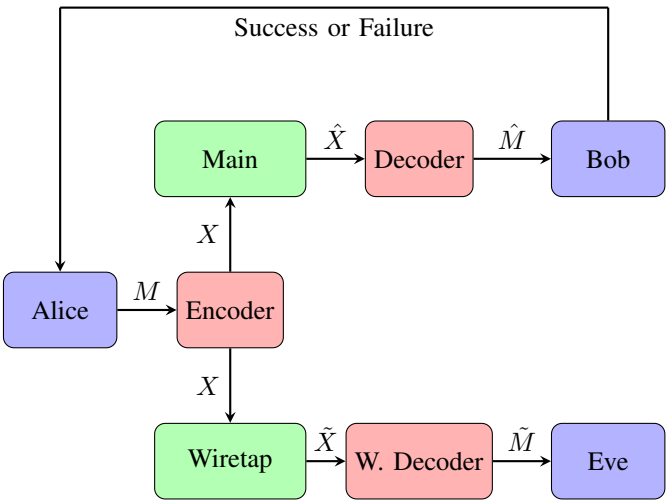

Fig. 1: Wiretap Channel Model With Feedback

where $f = \frac{c}{\lambda}$ is the transmit frequency, c the speed of light, λ is the wavelength, t is time, and δt is the time delay needed to achieve the phase shift $\alpha = 2\pi f \delta t$. If θ is the angle toward a receiver off the positive x-axis, then we have

$$\begin{aligned} \sin(\theta) &= \frac{c\delta t}{\frac{\lambda}{2}} \\ &= \frac{\frac{c\alpha}{2\pi f}}{\frac{\lambda}{2}} \\ &= \frac{c\alpha}{\pi f \lambda} \\ &= \frac{c\alpha}{\pi c} \\ &= \frac{\alpha}{\pi} \\ \Rightarrow \alpha &= \pi \sin(\theta) \end{aligned}$$

Thus, if we want to steer the beam in the direction θ, we need a phase shift of $\pi \sin(\theta)$ from one antenna to the next. So we weight the output of each antenna by $e^{\alpha k i} = e^{\pi \sin(\theta) k i}$ where k is the index of the antenna (in this case, from bottom to top, starting with 0, with the origin of our system is located at the middle of the antenna array). For all transmissions, we will assume that Alice and Bob have already established a connection as outlined in REFERENCE DATBLRF so that Alice knows the optimal phase shift to Bob, which we will place in the direction perpendicular to Alice's antenna array, or rather, in the direction of $\theta = 0$ on a polar graph. Alice then calculates the half power beam width, which is the two angles on either side of the optimal angle that receive half the power of the main angle. This gives her an angle range $[\theta_{min}, \theta_{max}]$ where, since Bob is oriented towards $\theta = 0$, we should have $\theta_{min} \approx -\theta_{max}$, so we choose $\phi = 2\theta_{max}$. An image providing the Signal-to-Interference and Noise Ratio (SINR) as for a beam directed at $\theta = 0$ can bee seen in Fig. 3.

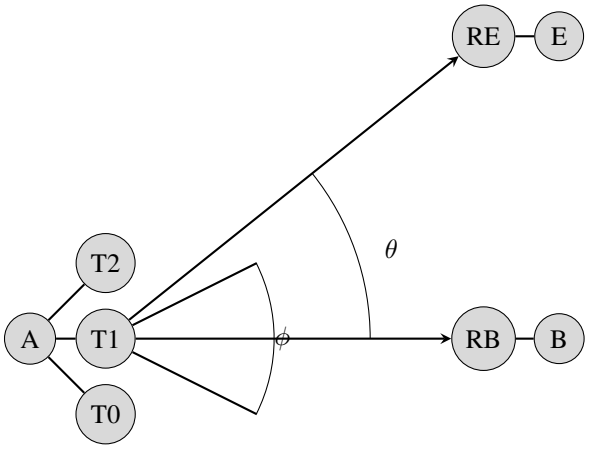

Fig. 2: An example of the transmission set-up where Alice utilizes three transmitters, and Bob and Eve both have one receiver.

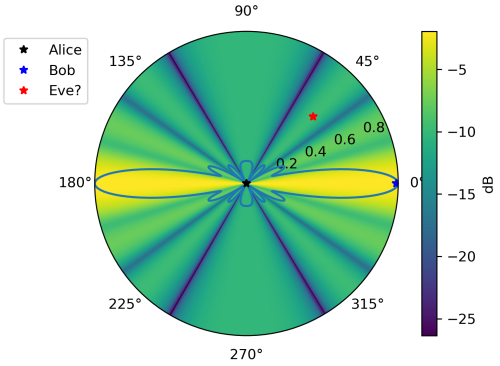

Fig. 3: SINR by Location

III. Impact of Randomized Beamforming on PEP

The main benefit of the beamforming is to take advantage of possible differences in the physical locations of Bob and Eve. If Eve is at a different enough angle from Alice than Bob that she is not in the main beam for the transmission of a specific packet, then the SINR at Bob will be much better than the SINR at Eve, making it more likely that Eve won't receive the packet but Bob will. While this is great if Eve truly is positions as in Fig. 3, it doesn't help very much if Eve is close enough to co-linear with Alice and Bob that she remains in the main beam of transmission as well as Bob. This is part of the reason for exploring the effect of randomization in the direction of the beam, as well as impairing the SINR inside the main beam of transmission. Since a beam pointed directly at Bob will result in the highest SINR being in the direction from Alice to Bob, if Alice just points the beam directly at Bob, then she is also pointing the beam directly at Eve. So, in this worst case scenario, how do we impair the transmission so that we can still achieve secrecy?

To answer that question, we should calculate what the optimal PEP should be from a secrecy probability standpoint. To do so, we consider the following optimization problem:

$$\begin{array}{ll} \max_{B_P, E_P} & B_P(1-E_P) \\ \text{s.t.} & E_P = B_P \\ & 0 \le E_P, B_P \le 1 \end{array}$$

where B_P, E_P is the probability that Bob and Eve receive a given packet respectively, as previously defined. The condition that $E_P = B_P$ comes from the fact that with this transmission scheme, we're guaranteed that for some packets in the transmission sequence (the exact number will be dependent on the random variable Φ) we will have $E_P \le B_P$. These are the packets we have the best chances of communicating secretly, so we focus on them. In this case, however, the worst case scenario is that $E_p = B_p$. Using Lagrange multipliers, it is easy to see that the solution to this problem is $B_P = E_P = \frac{1}{2}$, so the most probable way to get Bob to receive a packet that gets erased on Eve's channel is if the minimum PEP inside the main beam is 50%. This is the minimum PEP because it is better for both Eve and Bob to drop the packet, than it is for both Eve and Bob to receive the packet. Every time Bob drops the packet, he will simply request a retransmission, which will give Eve another shot at receiving the packet, essentially making it equivalent (security wise) to a situation where we just haven't transmitted that packet yet. If they both receive it, however, than we've already leaked information to Eve. Since the goal for these first few patterns is to achieve security, in a choice between Eve receiving a packet or Bob dropping a packet, we prefer to have Bob drop the packet.

In a SISO channel where Alice has multiple antennas and there is Rayleigh fading, the received signal is

$$y = \sqrt{P}\mathbf{h}^H\mathbf{w}s + n \tag{2}$$

where $\mathbf{h} = \begin{bmatrix} h_0 & \dots & h_{N-1} \end{bmatrix}^T$ with $h_k \in \mathscr{CN}(0, \sigma_h^2)$, $n \in \mathscr{N}(0, \sigma_n^2)$, and P is the power of the signal in Bob's direction. Thus, the SINR is defined as

$$\Gamma = \frac{P}{\sigma^2}\left|\mathbf{h}^H\mathbf{w}\right|^2 \tag{3}$$

For simplicity, we will assume that both the Rayleigh fading and the Additive White Gaussian Noise (AWGN) have mean 0 and unit variance, that is $\sigma_h = \sigma = 1$. From this SINR and the the assumption that we will transmit with Quadrature Phase-Shift Keying (QPSK), we then can directly calculate the Bit-Error Rate (BER) as $Q(\sqrt{2\Gamma})$ where

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{u^2}{2}}\,\mathrm{d}u \tag{4}$$

Finally, if it is possible to correct t bit errors in a packet of M bits, then the PEP is the probability that we have at least $t+1$ errors, or rather

$$\Psi = \sum_{i=t+1}^{M}\binom{M}{i}\epsilon_c^i(1-\epsilon_c)^{M-i} \tag{5}$$

We will consider the packet as corrupted (and thus discard it) if any bit is received in error, thus

$$\begin{aligned}\Psi &= \sum_{i=1}^{M} \binom{M}{i} \epsilon_c^i (1-\epsilon_c)^{M-i} \\ &= 1 - \binom{M}{0} \epsilon_c^0 (1-\epsilon_c)^M \\ &= 1 - \left(1 - Q\left(\sqrt{2\Gamma_c}\right)\right)^M \\ &= 1 - \left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\sqrt{2\Gamma_c}} e^{-\frac{u^2}{2}}\, \mathrm{d}u\right)^M\end{aligned}$$

While this is obviously ideal, the SINR will vary from transmission to transmission, and as such, there is no way to guarantee that PEP is always 50%. However, through careful transmission selection, a code can be designed to put the average PEP for the best location (which is Bob's position) near 50%.

With this, we now have to consider which distributions we should use as random variables in order to determine which directions we point the beams. As stated before, the obvious choice is to not include a random variable, and just point all the beams directly at Bob to transmit the packets. However, the question we want to answer is whether or not choosing a random variable to distribute the beam directions will help increase secrecy, without damaging the reliability. In this paper, we consider three different distributions: a uniform distribution, a truncated normal distribution, and a sinusoidal distribution. Since these are a function of ϕ, for the uniform distribution, we have

$$\Phi_U(x,\phi) = \begin{cases} \frac{1}{\phi} & -\frac{\phi}{2} \le x \le \frac{\phi}{2} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

the truncated normal distribution is defined as

$$\Phi_{TN}(x,\phi) = \begin{cases} \frac{e^{-x^2/2}}{\sqrt{2\pi}\left(1-2Q\left(\frac{\phi}{2}\right)\right)} & -\frac{\phi}{2} \le x \le \frac{\phi}{2} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

and the sinusoidal distribution as

$$\Phi_S(x,\phi) = \begin{cases} \frac{1-\cos\left(\frac{2\pi}{\phi}x\right)}{\phi\left(1-\frac{1}{\pi}\sin\left(\frac{2\pi}{\phi}\right)\right)} & -\frac{\phi}{2} \le x \le \frac{\phi}{2} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

While many values of ϕ were chosen, the most interesting are $\phi = 0$, and when ϕ is the half-beam width of the beam directly pointed at Bob, which in this case, was $\phi = \frac{\pi}{18}$.

IV. Results and Analysis

To achieve these results, numbers were calculated as if using 7 transmitting antennas oriented vertically, with a single receiving antenna. These numbers were calculated for 500 different points evenly spaced on a circle of unitary distance from the transmitter. Each of the 100 packets was set to be 10 bits long, and transmitted at the same power level, without any encoding (though those numbers were included in coding so

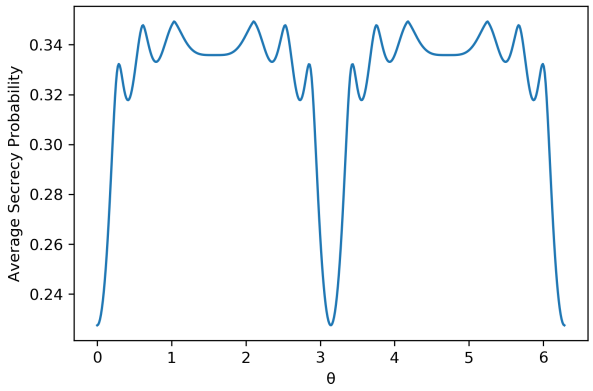

Fig. 4: Secrecy Probability: The overall probability that Bob receives a packet Eve drops that packet $\phi = 0$ (so all distributions are the same).

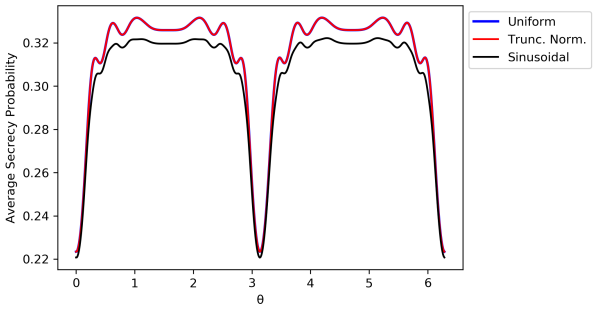

Fig. 5: Secrecy Probability: The overall probability that Bob receives a packet Eve drops that packet $\phi = \pi/18$. In order, Uniform, Truncated Normal, and Sinusoidal

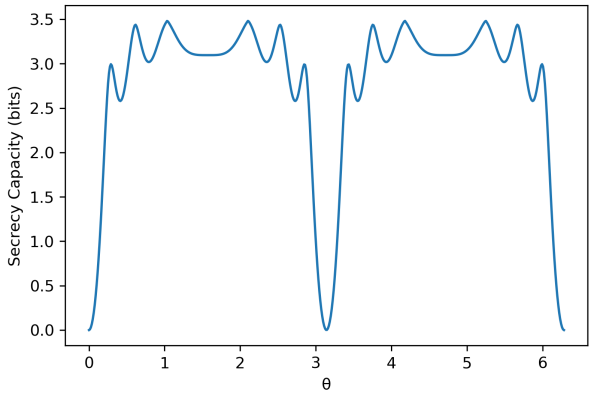

Fig. 6: Secrecy Capacity: The approximate number of bits we can secretly transmit to Bob per channel use (which sends 10 bits) and a range of $\phi = 0$ (so all distributions are the same).

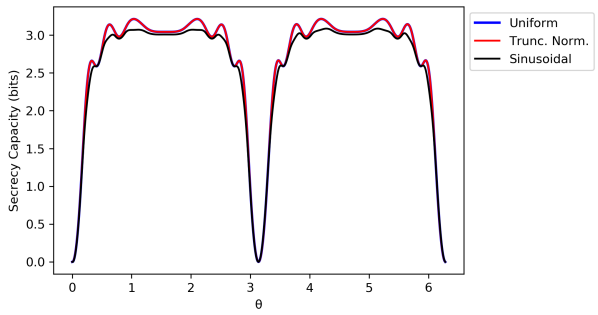

Fig. 7: Secrecy Capacity: The approximate number of bits we can secretly transmit to Bob per channel use (which sends 10 bits) and a range of $\phi = \pi/18$. In order, Uniform, Truncated Normal, and Sinusoidal

that they can be adjusted). The probabilities were calculated using 1000 simulations of transmitting these packets.

In Fig 4 and Fig 5, we have a graph of the secrecy probability as a function of θ. Fig 4 is this probability when transmission beams are directed at Bob, and only Bob, while Fig 5 is the probabilities when transmission beams are randomly selected from within the half-beam width of the beam pointing directly at Bob. In the progression from $\phi = 0$ to $\phi = \frac{\pi}{18}$, the probability decreases on average by 1%, from approximately 33% to approximately 32% at best and 23% to 22% at worst. This decrease happens at a more or less steady pace, and continues to decrease as ϕ extends further outside the half-beam width. This is reflected rather accurately in the figures representing the secrecy capacity graphs in Fig 6 and Fig 7 (both of which are a measurement of secrecy capacity as a function of θ). As we can see, utilizing beamforming to increase security at the physical layer is feasible, and can allow for security to be improved strictly by the angle from Bob to Eve, Unfortunately, none of the random distributions actually improved the security. However, what this scheme doesn't account for, and can be continued in later work, is the possibility of using the random distributions to determine pointing the antenna in different directions while maintaining the central beam pointed directly at Bob. This process could provide the added secrecy that this simple scheme did not.

V. Conclusion

While this scheme is obviously very rough and not very advanced, it does indicate that transmission security can be improved by utilizing beamforming, without decreasing reliability. Just by utilizing beamforming, we can have the probability for Bob receiving a packet that Eve drops around 30%, and get an average secrecy capacity of 2.78 bits per 10 bit channel use. Randomizing the beamforming direction does not seem to increase the secrecy of the transmission at this simpler level, but further explorations will be needed to fully rule this out as a useful schematic.

Coupled with the security themes in [1], this scheme can improve security for the physical layer against attackers using publicly available off the shelf equipment.

References

[1] W. K. Harrison, J. Almeida, D. Klinc, S. W. McLaughlin, and J. Barros, "Stopping sets for physical-layer security," in *Proc. IEEE Information Theory Workshop (ITW)*, Aug. 2010, pp. 1–5.

[2] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, "Coding for cryptographic security enhancement using stopping sets," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 575–584, Sep. 2011.