Creating Secrecy Through Erasure Channels

Panagiotis Kostopoulos

I&C, EPFL

Abstract—Security is one of the most important issues in communications. Security issues arising in communication networks include confidentiality, integrity, authentication, and non-repudiation [1]. We exclusively study confidentiality issues and consider the problem of generating over wireless channels a shared secret key $S$ between two parties, in the presence of an eavesdropping adversary. We focus on information theoretic approaches that, in contrast to existing cryptographic solutions, aim to provide security without making any assumptions about the adversary’s computational capabilities. We first consider the wiretap channel and show that secret communication is possible if the eavesdropper’s channel has a smaller capacity than the legitimate receiver’s channel [2]. Next, we describe a protocol that guarantees secrecy using artificial noise [3] and also present a practical method that actively secures wireless channels using zero-forcing beamforming [4]. Finally, we present preliminary results of a practical framework for secret key generation that creates erasure channels using wiretap codes and builds on computationally efficient techniques from network coding [5].

Index Terms—secret key agreement, erasure channels, wiretap codes, information theoretic security, secrecy.

I. INTRODUCTION

The proliferation of wireless networks and their inherent insecurity, due to the broadcast nature of the medium, has recently brought the issue of confidentiality (or secrecy) into the spotlight. The typical scenario is two users, Alice and Bob, who wish to exchange a message and keep it secret from an eavesdropper, Eve. Traditionally, cryptographic schemes, such as public-key cryptography, have been proposed to guarantee secrecy and their successful operation relies on certain unproved assumptions regarding computational complexity classes (hence, these schemes achieve “conditional secrecy”). In contrast to this, information-theoretic (or unconditional) secrecy, which was introduced in the pioneering work of Shannon [6], is based on the notion that it is possible to properly encode the message so that Eve does not gain any information about it in the first place, even with infinite computational resources.

The idea of generating information theoretic secrecy through erasure channels, (which admit a tractable theoretical analysis) has been proposed in the past. In fact, there has been a lot of relevant work in the secrecy context on top of erasure channels [7], [8]. Hence, if we could transform the wireless channels into erasures, we could benefit from these prior works. We can exploit channel variability to effectively create erasure channels using wiretap codes; the latter ensure that any node, including Eve, completely misses some fraction of the transmitted packets (i.e. it gets zero information about them), so that the packets are effectively “erased”.

Erasure channels do not occur naturally: even if we ensure that some fraction of the transmitted packets are corrupted by noise at Eve’s receiver, there is still a non-negligible probability that Eve can extract some useful information from them. Wiretap codes enable us to make this probability arbitrarily small, i.e they ensure that, as long as Eve’s signal-to-noise ratio (SNR) is below a given threshold, she can extract zero information from the received packets.

We first present the pioneering work of Wyner [2], who introduced the wiretap channel, defined the notion of secrecy capacity and showed that, if Eve’s channel is “worse” than Bob’s, a secret message can be hidden in the noise difference between them. Next, we describe how we can make Eve’s channel a degraded version of Bob’s (with high probability) and so guarantee secrecy [3]. Moreover, we examine a practical approach towards building practical information theoretically secure systems [4].

Finally, we present a system that leverages the above to enable $n$ wireless nodes to create a shared secret $S$, in a way that an eavesdropper, Eve, obtains no information on $S$. Our system
consists of two steps: (1) The nodes transmit packets, such that there exists a group of transmitted packets for which Eve has no information. This is achieved through a combination of beamforming by physically rotating the transmitting antenna (from many different sources) and wiretap codes. (2) The nodes participate in a protocol that reshuffles the information known to each node, such that the nodes end up sharing a secret that Eve knows nothing about.

II. THE WIRETAP CHANNEL

The wiretap channel, shown in Fig. 1, is the simplest non-trivial physical layer model that captures the problem of communication security. Denote the first $K$ source bits as $S^K = (S_1, ..., S_K)$. The encoder produces a vector $X^N = (X_1, ..., X_N)$, which is the input of the main channel. The output of the main channel is a vector $Y^N = (Y_1, ..., Y_N)$ which is also the input of the wiretap channel. Moreover, the output of the wiretap channel is the vector $Z^N = (Z_1, ..., Z_N)$ and the observed binary data stream after the decoder is the $K$ bits sequence $\hat{S}^K = (\hat{S}_1, ..., \hat{S}_K)$. We assume that the wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver. The objective is to maximize the rate of reliable communication from the source to the legitimate receiver, subject to the constraint that the wiretapper learns as little as possible about the source output. The achievable rate equivocation region is determined when both channels are discrete memoryless channels without feedback. It is shown that, in most cases, there exists a secrecy capacity $C_s > 0$ such that by operating at rates below $C_s$, it is possible to ensure that the wiretapper is essentially no better informed about $S^K$ after observing $Z^N$, than he was before.

A. System Model

We consider a discrete memoryless source which is characterized by its entropy $H(S)$. The two channels “main and wiretap” are discrete memoryless. Since the main channel is memoryless and used without feedback, the transition probability for $N$ vectors is

$$Q_M^{(N)}(y|x) = \prod_{n=1}^{N} Q_M(y_n|x_n).$$

The cascade of the main and the wiretap channels is also a memoryless channel with transition probability:

$$Q_{MW}(z|x) = \sum_{y \in Y} Q_{W}^{(N)}(z|y) Q_{M}^{(N)}(y|x).$$

The transmission rate $R$ is $KH(S)/N$ source bits per channel input symbol. The equivocation rate of the source at the output of the wiretap channel is:

$$\Delta = \frac{1}{K} H(S^K|Z^N) = H(S) \frac{H(S^K|Z^N)}{H(S^K)},$$

which expresses the uncertainty the wiretapper has after observing $Z^N$ and is used as the basic secrecy metric in this system. We also consider the average probability of erroneous decoding which is defined as follows:

$$P_e = \Pr(S^K \neq \hat{S}^K) = \frac{1}{K} \sum_{k=1}^{N} \Pr(S_k \neq \hat{S}_k).$$

The main problem is to determine the set $\mathcal{R}$ of achievable $(R, d)$ pairs where, by definition, $(R, d)$ is achievable iff for all $\epsilon > 0$ there exists an encoder-decoder such that

$$\frac{(H(S)K)}{N} \geq R - \epsilon,$n

$$\Delta \geq d - \epsilon,$n

$$P_e \leq \epsilon.$$n

Given the above channels $Q_M$, $Q_W$ and $Q_{MW}$, we consider the input random variable $X$, while $Y$ is the output of channel $Q_M$ and $Z$ the output of channel $Q_{MW}$. For $R \geq 0$, let $\mathcal{P}(R)$ be the set of pdfs $p_X(x)$ such that $I(X; Y) \geq R$. For $0 \leq R \leq C_M$, we define:

$$\Gamma(R) = \sup_{p_X \in \mathcal{P}(R)} I(X; Y|Z).$$

For any distribution $p_X$ on $X$, the $X$, $Y$, $Z$ form a Markov chain in that order. So,

$$I(X; Y|Z) = H(X|Z) - H(X|Y, Z) = H(X|Z) - H(X|Y) = I(X; Y) - I(X; Z).$$

Finally, we take:

$$\Gamma(R) = \sup_{p_X \in \mathcal{P}(R)} [I(X; Y) - I(X; Z)].$$

The first main contribution of Wyner’s work is summarized in the following Theorem, which defines the capacity-equivocation region of the wiretap channel:

**Theorem 2:** The set $\mathcal{R}$ of achievable rate-equivocation is given by

$$\mathcal{R} = \{(R, d) : 0 \leq R \leq C_M, 0 \leq d \leq H(S), Rd \leq H(S) \Gamma(R)\}.$$
as shown in (3). In this setting, the highest secure transmission rate of the system is:

\[ C_s = \max_{(R, H(S)) \in \mathcal{R}} R. \] (11)

\( C_s \) is called the “secrecy capacity” of the wiretap channel.

The second main contribution of this work is as follows. Since the wiretap channel \( Q_{MW} \) is a degraded version of the main channel \( Q_M \), the following theorem is true:

**Theorem 3:** If \( C_M > C_{MW} \), there exists a unique solution \( C_s \) of the equation \( \alpha = \Gamma(\alpha) \). Furthermore, \( C_s \) satisfies

\[ 0 < C_M - C_{MW} \leq \Gamma(C_M) \leq C_s \leq C_M \] (12)

and \( C_s \) is the maximum \( R \) such that \((R, H(S)) \in \mathcal{R}\).

**Theorem 3** essentially guarantees perfectly secret communication between the transmitter and the legitimate receiver at a non-zero rate \( C_s \).

The third main contribution of Wyner is the idea of performing random encoding for guaranteeing secrecy. This is actually the way of proving the direct part of **Theorem 2**. We use multicochannel and a two-step randomized encoding scheme to help hide the message from the eavesdropper [9]. Denote as \( S^K \) the message that we want to communicate to the legitimate receiver. The first step is to partition the codebook in \( 2^{NR} \) subcodebooks. This partition is known to Eve. The next step of the encoding is to select randomly and uniformly over each subcodebook (based on the message \( S^K \)) which of the \( 2^{NR} \) codewords we will send.

\[ X^N = f(S^K, l), \] (13)

where \( l \) is a randomly selected integer in the range \((1, 2^{NR} - R)\). More precisely, for each message \( S^K \), we generate a subcodebook \( C(S^K) \) consisting of \( 2^{NR} - R \) sequences \( X^N(l) \), where \( R \) is an encoding control parameter. To send \( S^K \), the encoder randomly chooses the \( X^N(l) \) sequence in its subcodebook and transmits it. The receiver can recover the index \( l \) if \( R \leq I(X; Y) \). For each subcodebook \( C(S^K) \), the eavesdropper has roughly \( 2^{NR} - R + I(X; Z) \) sequences such that \((X^N(l), Z^N)\) are jointly typical. Thus, if \( R > I(X; Z) \) the eavesdropper has a roughly equal number (in the exponent) of jointly typical sequences from each subcodebook and, hence, has almost no information about the actual message sent. This is the (direct) proof of achievability for **Theorem 2**.

### III. Guaranteeing Secrecy Using Artificial Noise

In this Section, we present a method of guaranteeing secrecy using artificial noise generated at the transmitter or with the help of dedicated relays (a similar approach is proposed in [10]). As we showed above, secret communication is possible if the eavesdropper’s channel has a smaller capacity than the receiver’s channel. Therefore, in order to make eavesdropper’s channel a degraded version of the receiver’s channel, the method proposed in [3] uses artificial noise. The notion of “secrecy capacity” is again defined as the largest rate that can be reliably communicated to the legitimate user such that the eavesdropper has zero information on the transmitted message.

\[ X_k = s_k + w_k, \] (16)

namely the information bearing signal \( s_k \) (selected by the transmitter as \( s_k = p_k u_k \), where \( u_k \) is the information signal and the power vector \( p_k \) is chosen such that \( H_k p_k \neq 0 \) and \( ||p_k|| = 1 \)) and the artificial noise signal \( w_k \). Both \( s_k \) and \( w_k \) are complex Gaussian vectors. Based on the fact that the
transmitter knows the legitimate receiver’s channel but not the eavesdropper’s channel, the artificial noise can be constructed so that it lies in the null space (i.e., \( H_k w_k = 0 \)) of the legitimate receiver’s channel, so that it holds \( w_k = Z_k v_k \), where \( Z_k \) is a matrix created by basis vectors in the null space and \( v_k \) are i.i.d complex Gaussian random variables with zero mean and variance \( \sigma_v^2 \). Under these assumptions, the signals received by the receiver and the eavesdropper, respectively, become as follows:

\[
z_k = H_k s_k + n_k, \\
y_k = G_k s_k + G_k w_k + e_k.
\]

Ideally, the eavesdropper’s channel should be a degraded version of the receiver’s channel so that we are able to hide the secret message. The secrecy capacity is lower bounded as

\[
\text{Secrecy Capacity} \geq C_{\text{sec}}^\alpha \geq I(Z; U) - I(Y; U) = \log \left( 1 + \frac{|H_k p_k|^2 \sigma_n^2}{\sigma_n^2} \right) - \log \left( 1 + \frac{|G_k p_k|^2 \sigma_n^2}{E|G_k w_k|^2 + \sigma_r^2} \right).
\]

(19)

\( C_{\text{sec}}^\alpha \) is a random variable, as it depends on the values of the random channel gains \( H_k \) and \( G_k \). Because of that, we study the average secrecy capacity and outage probability. The total transmit power is given by \( f_1(\sigma_n^2, \sigma_r^2) = E|\beta_k x_k|^2 = \sigma_n^2 + (N_T - 1) \sigma_r^2 \) and is upper bound by \( P_0 \). We can choose such \( \sigma_n^2, \sigma_r^2 \) in order to maximize the lower bound on average secrecy capacity,

\[
\hat{C}_{\text{sec}} = \max_{f_1(\sigma_n^2, \sigma_r^2) \leq P_0} \mathbb{E}[H_k] C_{\text{sec}}^\alpha.
\]

(20)

The worst case for the secrecy scenario occurs when the eavesdropper is much closer to the transmitter than the receiver. The minimum guaranteed secrecy capacity for the first scenario is given by the following relationship:

\[
\tilde{C}_{\text{sec}} \geq C_{\text{sec}, \text{mg}}^\alpha = \max_{f_2(\sigma_n^2, \sigma_r^2) \leq P_0} \mathbb{E}[H_k] \mathbb{G}_k \left( \log \left( 1 + \frac{|H_k|^2 \sigma_n^2}{\sigma_n^2} \right) - \log \left( 1 + \frac{|G_k|^2 \sigma_n^2}{(G_k Z_k Z_k^H G_k^H) \sigma_r^2} \right) \right).
\]

(21)

Based on (19), the best case for the secrecy scenario is when \( \sigma_n^2 \rightarrow \infty \) so that \( C_{\text{sec}} \) approaches the (unsecure) capacity of the main channel. On the other hand, when \( \sigma_n^2 \rightarrow 0 \), \( C_{\text{sec}} \)

approaches a non-zero value \( C_{\text{sec}, \text{mg}}^\alpha \), as we can observe in Fig. 4.

C. Scenario 2

In this scenario, the transmitter does not have multiple transmit antennas. The transmitter \( A \), the legitimate receiver \( B \) and the passive eavesdropper \( E \) each has a single antenna. There exist several relays \( (H_1, H_2, ..., H_{N_R}) \) which simulate the effect of multiple transmit antennas. The channel gain from node \( X \) to node \( Y \) is denoted as \( \alpha_{XY} \), where \( \alpha_{XY} \neq \alpha_{YX} \). A 2-stage protocol is implemented, which performs the coordination between the transmitter and the relays. In the first stage, both the transmitter and the legitimate receiver transmit independent artificial noise signals to the relays so that the received signals are:

\[
r_{H_i} = \alpha_{AH_i} \alpha_{ABX} + \alpha_{BH_i} y + n_i, \\
r_{E,1} = \alpha_{AE} \alpha_{ABX} + \alpha_{BE} y + e_1,
\]

(22)

(23)

where \( x, y \) are Gaussian random variables with variance \( \sigma_x^2, \sigma_y^2 \), respectively.

In the second stage, the relays relay a weighted version of the signal that they receive using weights that may be known to the eavesdropper. Concurrently, in the second stage, the transmitter sends its secret message \( z \). The receiver (due to his knowledge) cancels the artificial noise component and receives the secret message the transmitter wants to communicate. The channel from \( A \) to \( E \) can be represented as follows:

\[
r_B = \alpha_{AB} z + n_B, \\
r_E = h_z z + H_{xy} \left( \begin{array}{c} x \\ y \end{array} \right) + n, \\
h_z = \begin{pmatrix} 0 \\ \alpha_{AE} \end{pmatrix}, \\
E = \begin{pmatrix} \sum_{i=0}^{N_R} \beta_i \alpha_{AH_i} E n_i + e_2 \end{pmatrix}, \\
H_{xy} = \begin{pmatrix} \alpha_{AB} \alpha_{AE} \gamma \\ \sum_{i=1}^{N_R} \beta_i \alpha_{AH_i} E \end{pmatrix},
\]

(24)

(25)

(26)

(27)

where \( \gamma = \alpha_{AB} \sum_{i=0}^{N_R} \beta_i \alpha_{AH_i} \alpha_{EH}, (e_1, e_2) \) are AWGN noise samples of variance \( \sigma_e^2 \) and \( \sigma_n^2 \) and \( \beta_i \) are (publicly known) i.i.d complex Gaussian random weights (used by the relays) of variance \( \sigma_{\beta_i}^2 \). The lower bound on secrecy capacity for this scenario is given by:

\[
C_{\text{sec}}^b = I(Z; R_B) - I(Z; R_{E,1}, R_{E,2}) = \log \left( 1 + |\alpha_{AB}|^2 \gamma^2 \sigma_n^2 / \sigma_{AB}^2 \right) - \log \left( |h_z h_z^* + K| / |K| \right).
\]

(28)

where \( \sigma_{AB}^2 = \sum_{i=0}^{N_R} (|\alpha_{AH_i}|^2 \sigma_{\beta_i}^2) \sigma_n^2 + \sigma_e^2 \). As in the previous scenario, \( C_{\text{sec}}^b \) is a random variable as a function of the random channel gains and its average value \( C_{\text{sec}}^b \) can be optimized over the power allocation as:

\[
\hat{C}_{\text{sec}} = \max_{f_2(\sigma_n^2, \sigma_r^2) \leq P_0} \mathbb{E}\log(1 + |\alpha_{AB}|^2 \sigma_e^2 / \sigma_{AB}^2) - \log \left( |h_z h_z^* + K| / |K| \right),
\]

(29)
Eavesdroppers (STROBE) [4] is a cross layer technique that are not generally able to guarantee secrecy. In this Section, techniques that do not know the location of the eavesdropper use of a directional transmission scheme. However, tech-
iques which are designed to exploit the location of the eavesdropper have the potential to create interference to potential eavesdroppers (E1−3). This framework exploits the ability of the Zero Forcing Beamforming (ZFBF) precoding method to create multiple simultaneous spatial streams.

D. Artificial Noise in MIMO Scenario

We now consider the scenario where all nodes, including the eavesdropper, use multiple antennas and present the results in [3] for the minimum guaranteed “MIMO secrecy capacity”. We consider the case where the number of antennas of the legitimate receiver and the eavesdropper is the same, i.e. $N_R = N_E$. The effect to the MIMO secrecy capacity of increasing the number of legitimate receiver antennas is not obvious. On one hand, there is the increase to the number of parallel channels and the ability to produce artificial noise. However, the eavesdropper also has more antennas, which requires artificial noise to be produced in more dimensions. As a result, there are fewer dimensions for transmitting information.

The lower bound on secrecy capacity is given by:

$$C_{\text{sec}} = I(Z; S) - I(Y; S)$$

$$= \log \left| I \sigma_s^2 + H_k Q_s H_k^H \right| - \log \left( \left| K + G_k Q_s G_k^H \right| \right),$$

where $Q_s = \mathbb{E}[s_k s_k^H]$. The transmitter should use at least $N_E$ dimensions for artificial noise generation. Let $N_{ND}$ the number of dimensions used for artificial noise $N_{SD}$ the number of dimensions used for information signal. The transmitter first chooses $N_{ND}$, where $N_E \leq N_{ND} \leq N_T - 1$.

We now define the notion of outage capacity as $Pr(C_{\text{sec,mg}} < C_{\text{outage}})$, where $C_{\text{outage}}$ is an outage capacity. We use $C_{\text{sec,mg}}$ to refer to both $C_{\text{sec,mg}}$ and $C_{\text{sec,mg}}$. We should highlight the fact that as $N_R$ increases which means that the number of parallel channels of the legitimate receiver increases, the outage probability reduces for small values of $N_R$. As $N_R$ becomes bigger and so $N_E$ becomes bigger, at most $N_T - N_E$ dimensions can be used for transmission and this has as a result the increase of the outage probability. The number of diversity paths plays a crucial role in the behavior of the outage probability.

IV. ACTIVELY SECURING WIRELESS COMMUNICATIONS USING ZERO-FORCING BEAMFORMING

A possible solution for secure wireless transmission is the use of a directional transmission scheme. However, techniques that do not know the location of the eavesdropper are not generally able to guarantee secrecy. In this Section, we present a technique that promises a solution to this problem. Simultaneous TRansmission with Orthogonally Blinded Eavesdroppers (STROBE) [4] is a cross layer technique that takes advantage of the multi-stream capabilities of existing technologies such as 802.11n for sending information to a legitimate receiver (LR) and concurrently creating interference to potential eavesdroppers (E1−3). This framework exploits the ability of the Zero Forcing Beamforming (ZFBF) precoding method to create multiple simultaneous spatial streams.

The main contributions of this work is an experimental comparison of STROBE with other candidate solutions for guaranteeing secrecy, which shows that STROBE achieves better security guarantees. An additional attractive feature of STROBE is that it is not affected by the eavesdropper’s proximity and orientation relative to the legitimate receiver. It is also demonstrated that the improved performance of STROBE depends crucially on the existence of strong multipath.

A. System Model and Experimental Platform

The experimental model consists of an $N$ antenna access point (AP) and $M$ users that have a single antenna each, as shown in Fig. 6. The channel vector for user $n$ is the $1 \times N$ row vector $h_n$ so that the channel matrix has dimensions $M \times N$ and is produced by concatenating the individual user’s row matrices. Also, there is an $N \times 1$ column vector $w_n$ which is the beamsteering vector of user $1, \ldots, M$. An $N \times M$ beamsteering matrix $W$ is also created. ZFBF selects weights that satisfy the zero-interference condition according to the following relationship

$$W = H^*(HH^*)^{-1},$$

where $*$ denotes conjugate transpose. Based on (30), we argue that the number of concurrent streams $M \leq N$. The “blinding streams” are produced at the same time with the transmission signal such that they are orthogonal to the transmitted signal. The orthogonality is achieved using the Gram-Schmidt process.

WARPLab is used for the experimental demonstration. WARPLab is a framework for rapid physical layer prototyping that allows for coordination of arbitrary combinations of single and multi-antenna transmit and receive nodes. The extensible framework gives users the flexibility to develop and deploy large arrays of nodes to meet any application or research need. All physical layer baseband processing takes place in MATLAB while the Over The Air (OTA) transmission and reception occur to the WARP nodes.

The schemes that are compared to STROBE performance wise are the following: (i) Ominidirectional Transmission: a benchmark scheme that employs a single omnidirectional antenna. (ii) Single-User Beamforming (SUBF): an adaptive scheme which only considers the channel to the legitimate
user (hence, it is agnostic to the eavesdroppers), so it can be considered as a special case of ZFBF. (iii) **Cooperative Eavesdropper** (CE): an unrealistic scheme where the transmitter learns the CSI of the eavesdroppers.

The **performance metric** is the Signal to Noise Ratio (\(SNR\)) or Signal to Noise plus Interference Ratio (\(SINR\)) expressed in dB. For a fair comparison among the schemes, the net transmit power is set to a fixed value for all of them regardless of the number of antennas or streams used.

**B. Experimental Results**

Fig. 7 shows the received \(SINR\) at each of the four receivers of the WLAN scenario in Fig. 6. Using an Omnidirectional antenna, we clearly observe greater \(SINR\) values at some eavesdroppers than at the legitimate receiver, due to their closer physical proximity. This is the main reason that existing systems cannot guarantee secrecy between a transmitter and a legitimate receiver. A better performance is observed for the case of using Single-User Beamforming. SUBF’s goal is to maximize the \(SINR\) at the legitimate receiver, but it tries to achieve that without considering the other locations. Hence, it is not surprising that \(E_3\) has a greater \(SINR\) than the legitimate receiver. Unlike the previous two schemes, we observe that the STROBE performs really well in such a WLAN scenario. It is clear that the key mechanism of orthogonal blinding gives STROBE the opportunity to minimize the \(SINR\) at the eavesdroppers while at the same time maximizing the \(SINR\) at the legitimate receiver. Finally, we compare STROBE’s performance with CE. We observe that the extra information available at the transmitter, regarding the channels of the potential eavesdroppers, is beneficial for completely blinding them, but also leads to a decrease in the legitimate receiver’s \(SINR\).

**Comparing STROBE with CE**

The CE scheme considers all users in order to create the blinding streams. As a result, it can completely blind \(N - 1\) eavesdroppers. In order to have a fair comparison between CE and STROBE, we consider only the case of four nodes. Both STROBE and CE generate their blinding streams using ZFBF. The only difference is that STROBE knows only the legitimate receiver’s channel whereas the CE knows the channel matrices of all receivers (including eavesdroppers). As a result, STROBE will always yield a higher \(SINR\) to the legitimate receiver because CE has to sacrifice some power in order to satisfy the zero-interference condition. We should mention that we do not show all the available figures for the experimental results in [4] due to lack of space.

**Eavesdroppers’ Location**

The work in [4] next examines how the distance of the eavesdropper (relative to the legitimate receiver) affects the schemes’ performance and also considers the special case when the eavesdropper is perfectly aligned with the legitimate receiver. In the Omnidirectional Transmission and Single-User Beamforming schemes, the presence of multipath leads to a small difference between the legitimate node and eavesdropper \(SINR\). In contrast, STROBE benefits from multipath effects and we observe a big difference between the \(SINR\) values of the legitimate receiver and the eavesdroppers. This means that STROBE is not vulnerable to the possible proximity of the legitimate receiver to the eavesdroppers.

We observe similar results when we place the nodes in a line. Specifically, the nodes are placed in a line where two of the eavesdroppers are closer to the transmitter than the legitimate receiver. The multipath effects are beneficial for STROBE’s performance whereas we take unpredictable results for the Omnidirectional scheme. The Single-User Beamforming scheme, being a directional scheme, produces the highest \(SINR\) at the node that is closer to the transmitter (which happens to be an eavesdropper). So based on that, we can argue that the best way to eavesdrop when the system uses SUBF is to put an eavesdropper in the LOS path of the legitimate receiver. In all cases, the performance of the CE scheme is close to that of STROBE. But as we mentioned before STROBE performs a higher \(SINR\) difference between the better eavesdropper and the legitimate receiver.

**Multipath Effects**

Based on the experimental results, the multipath effects are really important for STROBE’s performance, which explains why STROBE and CE perform successfully regardless of the relative position of any eavesdropper with the legitimate receiver. This is confirmed by repeating these experiments in an outdoor environment, where STROBE’s performance is completely different (worse, actually) and is very susceptible to the eavesdroppers’ position and separation distance.

**Powerful Eavesdropper**

Finally, an experiment is performed where a nomadic eavesdropper tries to find the best possible location for eavesdropping in an indoor environment. A big classroom, with a transmitter and 24 different positions for the eavesdroppers, is considered. For the Omnidirectional scheme we observe again that, due to the multipath effects, there is no dependence between the distance from the transmitter and the received \(SINR\). Hence, it is possible for the nomadic eavesdropper to find a suitable place in the room where she will achieve a high \(SINR\) value compared to the \(SINR\) value of the legitimate receiver. Similarly, for the Single-User beamforming scheme the multipath effects and existence of side lobes imply a lack of correlation between eavesdropper’s location and overheard signal strength; hence, SUBF can be defeated by a nomadic eavesdropper that performs an exhaustive search for the best possible location inside the room. Unlike the previous two schemes, STROBE exploits the benefits of the multipath effects and successfully blinds eavesdroppers in all possible
locations inside the room.

Because of the number of receivers (> 3), the scheme that we use for comparison with STROBE is a directional antenna scheme and not the CE scheme. Since the directional antenna focuses most of its energy inside the main beam, it is easy for the eavesdropper to find a suitable location inside the beam with a high SNR value. Hence, we conclude that, of all examined schemes, only STROBE can resist a determined eavesdropper that tries to search for an opportune eavesdropping location inside the room. Based on the above experimental results, we conclude that STROBE is a possible method for guaranteeing wireless security which can be easily built on top of existing wireless technologies.

V. PRELIMINARY RESULTS

In this Section, we present our preliminary results [5] for a system that leverages the limited network presence of the adversaries, to enable n wireless nodes (a.k.a terminals) to create a shared secret S, in a way that the eavesdropper, Eve, obtains very little information on S.

A. Protocol Description

Phase 1

Our secret agreement protocol assumes erasure channels between the legitimate nodes (terminals) and Eve. Since erasure channels do not occur naturally, the terminals use 2-layer wiretap codes to emulate them. Such a code is characterized by 2 parameters, SNR1 and SNR2. While Alice transmits using such a code, it is guaranteed that Bob will receive a message for which Eve has zero information, as long as Bob’s SNR is above SNR1 and Eve’s SNR is below SNR2. In this sense, wiretap coding translates SNR differences into erasures.

The main idea is the following: when Alice transmits, as she rotates her beam, there exists some time interval during which Bob will be inside Alice’s main antenna lobe, while Eve will be outside the lobe. Suppose we could guarantee that, during this time interval, Bob’s SNR is above SNR1, while Eve’s SNR is below SNR2. To achieve this, we set SNR1 to the average SNR that Bob experiences when inside Alice’s main lobe, and we set SNR2 to the best SNR that Eve experiences when outside the lobe. We also note that increasing SNR1 − SNR2 has two effects that tend to counteract each other. Specifically, although the rate of the wiretap code is increased, the probability that Bob’s SNR is above SNR1 and Eve’s SNR below SNR2 is decreased.

Since the actual secret rate depends on both factors, there exists a set of optimal SNR1, SNR2 values which can be used.

Phase 2

We now move to phase 2 of the system, which is actually the secret agreement protocol. At a high level: Alice first agrees on a pairwise secret Si with each legitimate node (a.k.a terminal) Ti, such that Eve knows nothing about Si. Once Alice has created a pairwise secret with each terminal, she could use these pairwise secrets to communicate a group secret to all the terminals. At the end of phase 1, the terminals have transmitted some number of packets (we will call them x-packets). Each terminal, as well as Eve, has received and knows the contents of some fraction of these x-packets.

The input to the secret agreement protocol in Phase 2 consists of:

1. The identities of x-packets known to each terminal.
2. A lower bound M1 on the number of x-packets shared by Alice and terminal Ti and missed by Eve.
3. A lower bound M on the number of x-packets shared by Alice and at least one other terminal and missed by Eve.

Pairwise Secret Algorithm

1. Alice (Ti) constructs linear combinations of the x-packets that she knows (we will call them y-packets) using a well-defined construction [11]. These y-packets satisfy two constraints:
   
   a) Their total number is M.
   b) M1 of them are linear combinations of the x-packets that Alice shares with terminal Ti̸=0. Alice reliably broadcasts the identities of the x-packets she used to create each y-packet.
   2. Each terminal (Ti̸=0) reconstructs the contents of M1 y-packets.

At this point, Alice and terminal Ti share M1 y-packets. The pairwise secret Si is their concatenation. The main idea is that in order to create a perfect pairwise secret with terminal Ti, Alice needs to know a lower bound of the number of x-packets shared with Ti and missed by Eve, and she must set M1 (the size of the pairwise secret) to this value.

Group-Secret Algorithm

The terminals now apply the following procedure:

1. Alice constructs \( M - \min\{M_1, M_2, \ldots, M_{n-1}\} \) linear combinations of the y-packets (we will call these z-packets), using a well-defined construction [5]. She reliably broadcasts both the contents of each z-packet and the identities of the y-packets used to construct each z-packet.
2. Each terminal Ti̸=0 reconstructs the \( \{M - M_1\} \ y \)-packets it is missing by combining any of the \( \{M - M_1\} z \)-packets with the \( \{M_i\} y \)-packets it reconstructed in step 2 of the Pairwise Secret algorithm.
3. Alice constructs \( L = \min\{M_1, M_2, \ldots, M_{n-1}\} \) linear combinations of the y-packets (we will call them s-packets), using a well-defined construction [5]. She reliably broadcasts the identities of the y-packets that she used to create each s-packet.
4. Each terminal is now able to reconstruct all the s-packets, because it has all the y-packets.

At this point, all terminals share the same set of L s-packets.
The group secret key $S$ is the concatenation of the $s$-packets.

### B. Evaluation

In this Section, we evaluate our system in terms of the quality of the secrets it generates (i.e., how much Eve knows about them) and the rate at which it generates new secrets. We evaluate our system on a small testbed of 5 WARP nodes, 4 of them acting as legitimate terminals and one of them acting as the eavesdropper Eve.

We are interested in measuring the secrecy rate achieved by our system and also the level of reliability of the generated keys. In other words, we are interested in knowing how well we can estimate how many packets Eve missed compared to what we could do if we were assisted by an Oracle system (a hypothetical entity that provides Eve’s SNR to the terminals). Hence, we define reliability as the ratio: (number of secret bits from Oracle)/(estimated number of secret bits). Ideally, we would like to achieve reliability $> 1$ (which actually occurs).

We also got some other interesting experimental results. First, we see that, although we change the positions of the terminals in our room, our channel conditioning results in a consistent performance (very similar efficiency and secrecy rate) for all the four topologies we tried. Indeed, the goal of our design is exactly that, to ensure that no matter where the terminals and Eve are located (provided they are separated by a certain distance) we can achieve a target secrecy rate. Moreover, in all experiments, our system achieves perfect reliability, as we create fewer secret packets than what the Oracle does. This is not a surprising result, given that our system goes to great lengths not to overestimate the amount of information collected by Eve. One question then is, how much does our conservativeness cost us in terms of secrecy rate? We also see that, in the worst case, our system achieves a minimum secrecy rate of 60Kbits/sec for $n = 4$ terminals. In contrast, Oracle achieves minimum secrecy rate more than 100Kbits/sec in the same scenario. The difference between our system and Oracle expresses how much we lose by not being able to estimate accurately the amount of information collected by Eve.

In summary, we show that, for a variety of node placements, the terminals agree on thousands of new secret bits per second. We verify that these bits are perfectly secret (Eve obtains no information about them) by measuring the mutual information between the signal that reaches Eve’s antenna and the signals that reach the antennas of the terminals. In other words, we ensure that Eve cannot learn anything about the shared secrets, even if she has access to corrupted packets that get discarded by the lower layers of her device. We should clarify that our system is designed to sacrifice secrecy rate in order to achieve high reliability. We prefer to produce fewer secret bits, but have higher confidence that Eve knows very little about them.

### VI. DISCUSSION AND RESEARCH PLAN

We first studied the notion of the wiretap channel, defined the notion of secrecy capacity and showed that if Bob has a better channel than Eve we can communicate a secret message from Alice to Bob [2]. Next, we presented a technique of making Eve’s channel a degraded version of Bob’s channel, using artificial noise, and as a result guaranteeing secrecy for any eavesdropper’s position [3]. Also, we examined a practical approach towards building practical information theoretically secure systems [4].

Along these lines, we presented preliminary results of a system that enables $n$ nodes, in a real wireless network, to create a shared secret $S$. To the best of our knowledge, there exists no solution (for 2 or more terminals) that does not require physical-layer changes, has been deployed on a real testbed, and has been experimentally shown to generate high-quality secrets in the presence of an adversary. The novelty of the system lies in the fact that it does not make any assumptions about Eve’s computational capabilities, but instead assumes that she has limited network presence.

Our system is not yet ready for deployment (we have evaluated it only on one testbed, with one adversary). However, it constitutes the first experimental evidence that it is feasible for a group of wireless nodes to agree on thousands of perfectly secret bits per second, without relying on the adversary’s computational limitations. Exploring the case where the adversary Eve has multiple receivers would be a natural future step of this work. Also, the evaluation of this protocol on top of other testbeds, and the consideration of different environments (indoor, outdoor) or room geometries would prove that our system is ready for deployment. It would also be interesting to examine the case where Eve can actively jam the communication and the legitimate users have to adapt the secret protocol to mitigate the jamming effect. Finally, the implementation of a commercial protocol that guarantees unconditional secrecy would be a goal that we can address as a challenge for future work.

### REFERENCES


