Everlasting Secrecy in Wireless Communications: Challenges and Approaches

*Dennis Goeckel**, *Azadeh Sheikholeslami*, and *Cagatay Capar*

Electrical and Computer Engineering Department, University of Massachusetts, Amherst, MA, USA, 01003,
Tel.: +1-413-545-3514, Fax: +1-413-545-4611, Email: goeckel@ecs.umass.edu,
sheikholesla@ecs.umass.edu,ccapar@ecs.umass.edu

Abstract

A guarantee of everlasting secrecy is of great interest in modern communication systems. Information-theoretic secrecy is a promising method for providing such and has been widely considered. However, the adoption of information-theoretic security has been hampered by the difficulty of guaranteeing the necessary conditions for secrecy to be realized in a wireless communications environment, where the adversary might have a significant (and likely unknown) signal-to-noise ratio (SNR) advantage over the intended recipient. Thus, whereas the wireless communications environment provides opportunities to gain an advantage over the adversary, as has been considered widely in the literature, it is that same environment that challenges its ultimate utility. We review pertinent past and emerging work to address these challenges and provide perspectives on future directions in the field.

1 Introduction

Security and privacy are critical concerns of modern communication systems. Here, we consider the achievement of everlasting secrecy, which we define as the content of a message being kept hidden indefinitely from a determined and capable adversary. In particular, the content of a message is often useful long after message transmission, and an adversary can record a signal and work to break the code indefinitely, yielding useful information years later [1].

The most commonly considered type of security, with nearly universal penetration in practical systems, is cryptographic security. In a cryptographic system, information is secured in such a way that a recipient holding the key has the ability to decipher the information, whereas the adversary, lacking the key, is faced with a "hard" problem which he/she is presumed to lack the computational capabilities to solve [2]. However, when considering everlasting secrecy, security based on computational assumptions of the eavesdropper becomes problematic. In particular, the adversary can record the transmission and work indefinitely to obtain the contents of the message. Success might come with significantly improved computation, weaknesses in the cryptosystem implementation, or the determination that the original primitive on which the system was based was not indeed hard.

This motivates information-theoretic security. In information-theoretic secrecy, the message is transmitted in such a way such that there is no leakage of the message to the adversary, even if that adversary is able to record the received signal and work on it indefinitely with unbounded computational power. Information-theoretic security originated with Shannon [3], who showed that the well-known one-time pad was the only way to reliably secure information *if* the adversary captured the ciphertext without distortion. This implied that the key need be as long as the message to be protected, thus requiring the distribution of long keys and making efficient one-way communication challenging.

Rather than assuming that the adversary had a clean look at the ciphertext, Wyner considered the case where the channel from the transmitter to the desired recipient is better than that to the eavesdropper [4]. This fits a commonly considered industrial espionage case, where you might have an eavesdropper outside the building (e.g. see Figure 1(a)). Whereas it might seem that this would simply lead to a higher bit error rate at the eavesdropper, Wyner demonstrated through the wiretap construction that one can actually send information at a positive rate while information-theoretic secrecy (i.e. no leakage of the message) is achieved.

After Wyner's work, other contributions (e.g. the consideration of the Gaussian channel [5] and the introduction of public discussion approaches [6], [7]), continued to be made at a relatively modest rate until the field became very active after in the millennium, when there was an explosion of interest in this strong form of secrecy applied to wireless channels. In particular, the channel of Figure 1(a) very much matches the Gaussian wiretap channel, and thus numerous groups began the consideration of security in wireless systems [8], [9].

However, despite the significant results that have been derived in information-theoretic security in wireless communication systems in the last decade, practitioners have been slow to warm to the notion. In particular, whereas the situation of Figure 1(a) fits the wiretap formulation, wireless channels are partially defined by node mobility and thus solving the difficult "near eavesdropper" problem (see Figure 1(b)) is paramount. Furthermore, in the case of a passive eavesdropper, the eavesdropper location might not be known, making rate selection and providing any security guarantees problematic. Hence, practitioners can rightly question whether information-theoretic security simply trades one type of risk (long-term computation risk) for another (short-term scenario risk), for which the latter seems more problematic.

In this paper, we overview this problem in detail in Section 2 and then present two emerging (and quite different) approaches for addressing this risk in Sections 3 and 4, respectively, before presenting our conclusions and perspectives on future directions of the field in Section 5.

This work has been supported by the National Science Foundation under Grants CNS-0905349, CNS-1018464, and CIF-1249275.

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

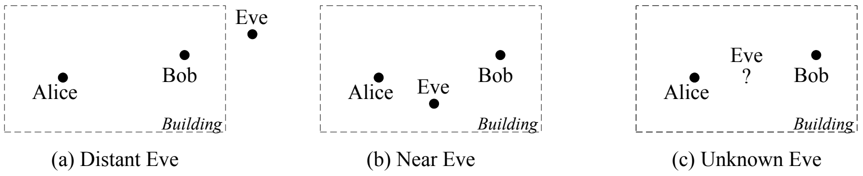


Fig. 1. Scenarios in the wireless environment, where the transmitter Alice attempts to transmit information secretly to the desired recipient Bob in the presence of an eavesdropper Eve: (a) the often envisioned scenario of Eve listening from the parking lot, where she has a significant disadvantage versus Bob; (b) the case where Eve is closer than Bob; and (c) the case where the location of Eve is unknown, which is likely for a passive eavesdropper.

2 System Model and Motivation

2.1 System Model

Consider a source Alice A, intended recipient Bob B, and eavesdropper Eve E, as shown in Figure 1. The i^{th} transmitted symbol of Alice will be denoted by $x_i^{(A)}$, and the i^{th} received symbol for Bob or Eve will be denoted by and $y_i^{(B)}$ and $y_i^{(E)}$, respectively. Assume a narrowband channel subject to frequency non-selective Rayleigh fading between each of the active transmitters and receivers. We assume slow block fading, where the fading affecting the transmission between any two nodes does not change during the course of that transmission. Then, the multipath fading on a link from a given transmitter X to a given receiver Y is a complex zero-mean Gaussian random variable and will be denoted as $h_{X,Y}$. Hence, the received signals at Bob and Eve will be given by:

$$y_i^{(B)} = \frac{h_{A,B}}{d_{A,B}^{\frac{\alpha}{2}}}\sqrt{E_s}x_i^{(A)} + n_i^{(B)}, \qquad \text{and} \qquad y_i^{(E)} = \frac{h_{A,E}}{d_{A,E}^{\frac{\alpha}{2}}}\sqrt{E_s}x_i^{(A)} + n_i^{(E)}, \tag{1}$$

where $d_{X,Y}$ is the distance between nodes X and Y, α is the path-loss exponent, E_s is the transmitted energy per symbol, and $\{n_i^{(B)}\}$ and $\{n_i^{(E)}\}$ are independent and identically distributed (i.i.d.) sequence of zero-mean (complex) Gaussian random variables with $E[|n_i^{(B)}|^2] = E[|n_i^{(E)}|^2] = N_0$. The Rayleigh fading assumption implies $|h_{X,Y}|^2$ is exponentially distributed with $E[|h_{X,Y}|^2] = 1$.

2.2 Motivation

Consider a simple scenario as shown in Figure 1. Given the model described in the previous section, the channel conditioned on the fading is a Gaussian wiretap channel; hence, it can support secure communication at a rate of [5]:

$$C_s = \max\left\{0, \frac{1}{2}\log\left(1 + \frac{E_s}{N_0}\frac{|h_{A,B}|^2}{d_{A,B}^{\alpha}}\right) - \frac{1}{2}\log\left(1 + \frac{E_s}{N_0}\frac{|h_{A,E}|^2}{d_{A,E}^{\alpha}}\right)\right\} \tag{2}$$

Critical to understanding the possibility of information-theoretic security is understanding the assumptions on the transmitter's knowledge of $d_{A,B}, h_{A,B}, d_{A,E}, h_{A,E}$. In particular, knowledge of $d_{A,B}$ and $h_{A,B}$ can be obtained through a simple protocol involving Alice and Bob, but obtaining $d_{A,E}$ and $h_{A,E}$ is more problematic.

Assume that $d_{A,B}$ and $h_{A,B}$ are known at Alice. If $d_{A,E}$ is known, then the transmitter Alice can use a desired secrecy outage probability ϵ to pick a rate R such that $P(C_s > R) = \epsilon$ [9]. However, if $d_{A,E}$ is small, the secrecy rate will be very small. More pertinently, if $d_{A,E}$ is unknown, or the eavesdropper enhances its reception through, say, a high gain receive antenna of unknown gain directed at the transmitter, it is impossible to guarantee even the secrecy outage ϵ. And, concerningly, if a secrecy outage occurs under this formulation, it is not simply that Bob did not get the message (i.e. the main channel capacity is too small), but rather that Eve did get the contents of the message (i.e. the eavesdropper channel capacity was too large), which implies a costly security breach.

3 Approaches at the Physical Layer

3.1 Background

When the main channel is at a disadvantage with respect to the eavesdropper channel, approaches based on public discussion [6], [7] can be applied to obtain a secret key between Alice and Bob. This key can then be used in a one-time-pad to convey a secret message. In order to be able to utilize public discussion strategies, the legitimate nodes should be able to perform two-way communication, and they require a noiseless, public, and authenticated channel. It is shown in [13] that, when the quality of Eve's channel is significantly better than the quality of Bob's channel, the secrecy capacity of public discussion drops rapidly. This fact motives us to seek other methods to provide secrecy.

Another way to combat an advantaged eavesdropper is to apply the approach introduced by Negi and Goel [11]. When the transmitter is equipped with multiple antennas, or some helper nodes for the legitimate nodes are available, artificial noise can be added to the signal such that the resultant artificial noise is placed in the null space of the legitimate receiver and thus does not affect it. On the other hand, the eavesdropper's channel will be degraded with high probability. This approach has been considered extensively in the literature; however, this method needs multiple antennas or helper nodes, which are not always available, and relies on interference cancellation, which can be challenging in a near-far situation.

3.2 Physical-Layer Intentional Distortion

We propose an approach to use inherent hardware imperfections of the eavesdropper's receiver to obtain physical layer security. We assume that Alice and Bob share a cryptographic key, which needs to be kept secret only until completion of the wireless transmission. Using this key, Alice distorts the transmit signal such that Eve would not be able to perform proper analog-to-digital conversion. Since Bob knows the key, he can cancel the distortion before his A/D and achieve a good signal for analog-to-digital conversion. In this case, even if the key is handed to Eve after time of transmission, she will not be able to extract the information from the recorded data. This approach can be used in several ways:

- Power modulation [12], [13]: at the transmitter, each symbol is multiplied by a gain which is taken from two random gains. Since Bob knows the key, he can put the reciprocal of the gain before his A/D, while Eve has to guess a gain. Hence, Eve loses information due to overflows of her A/D or high quantization noise. The risk to this scheme is an Eve with two A/Ds.
- Artificial intersymbol interference (ISI) [14]: motivated by the fact that the capacity of an AWGN channel is greater than the capacity of an ISI channel, Alice sends the signal through an artificial ISI filter, where the gains of the ISI filter are chosen based on the shared-key between Alice and Bob. Thus, Bob can equalize the received signal before his A/D to cancel the ISI, while Eve will not be able to do such and thus she will lose information.
- Random jamming [15]: Alice uses the key to select a random jamming signal (with large variations) and adds it to the signal that she wants to convey secretly. Bob will subtract the jamming signal before his A/D, while Eve cannot and thus she will have difficulty in matching her A/D span to the received signal. Hence, she will miss symbols due to A/D overflows, or she will lose information due to high quantization noise.

4 Using the Network

As can be seen from Sections 2.2 and 3, it is challenging to obtain physical layer security in the Alice-Bob-Eve scenario on wireless channels. Recently, there has been an approach to obtaining security in (asymptotically) large wireless networks detailed in [16]–[18]. Here, we briefly discuss the pertinent aspects of that work that would allow for the provisioning of security in practical (small to medium scale) wireless networks.

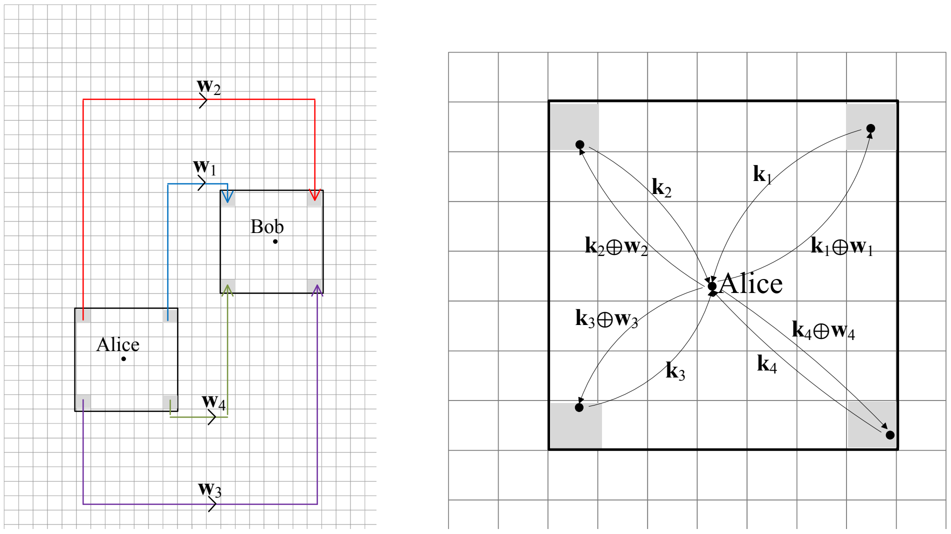
The two key techniques of [16]–[18] are summarized in Figure 2. First, the adoption of "secret sharing" [10] is important. Let $\mathbf{m}$ be the length-N binary message that we want to transmit. Before transmission, we randomly generate $M-1$ length-N binary "keys" $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{M-1}$. Then, we form the set of M length-N binary strings $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{M-1}$ and

$$\mathbf{w}_M = \mathbf{m} \oplus \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus \ldots \oplus \mathbf{w}_{M-1}. \tag{3}$$

The key observation is that a recipient must obtain all M binary strings from this set in order to decode the message. In particular, even if an eavesdropper misses a single string, that eavesdropper will obtain no information about the contents of the message. Thus, the construction must attempt to make sure that any eavesdropper, regardless of position, is unable to get all M binary strings. First, at the network layer, routing is done as shown in Figure 2(a). In particular, after exiting the local neighborhood of a given source node, routes, each carrying a different one of the M binary strings, are kept geographically separate so that a single eavesdropper cannot obtain multiple strings.

Next, consider how to protect at least one of the M binary strings from any eavesdropper in the area around the source. Let $M = 4$. One of each of the four binary strings will be sent to a node at each corner. But, if this were done by simply broadcasting the strings, an eavesdropper nearer to the source than the corners of the region would intercept all four strings. Consider the following solution. For the transmission of a string $\mathbf{w}_i$ to a given corner, first let the node in that corner (the eventual recipient) generate a random length-N binary vector $\mathbf{k}_i$ and transmit it to the source using Wyner's wiretap coding. Then, the source forms $\mathbf{k}_i \oplus \mathbf{w}_i$ and transmits the result using Wyner's wiretap coding. Now, to intercept the i^{th} binary string, an eavesdropper must be within the region but closer to the corresponding corner than the source. Since no eavesdropper, can be simultaneously closer to all four corners than the source, the system has a geographical advantage over Eve for at least one of the four strings and information-theoretic security can be realized [17], [18].

When considering finite networks as shown in Figure 1, such an approach could be performed in a densely populated office building, hence guaranteeing the presence of the nodes required to run the protocol. However, if such a density were not present, one could instead install fixed relay points in the corners of the area to be secured to facilitate with initial wireless transmission near every source.


$\mathbf{w}_2$
$\mathbf{w}_1$
Bob
Alice
$\mathbf{w}_4$
$\mathbf{w}_3$
$\mathbf{k}_2$
$\mathbf{k}_1$
$\mathbf{k}_2 \oplus \mathbf{w}_2$
$\mathbf{k}_1 \oplus \mathbf{w}_1$
Alice
$\mathbf{k}_3 \oplus \mathbf{w}_3$
$\mathbf{k}_4 \oplus \mathbf{w}_4$
$\mathbf{k}_3$
$\mathbf{k}_4$

(a) Routing

(b) Initiation at the source

Fig. 2. (a) M binary strings ($M = 4$ above) are generated and carried from the source node to the destination node with the help of relay nodes. Each binary string is carried on a separate path. The paths are chosen to be distant such that outside the source's and the destination's immediate neighborhoods, no eavesdropper can be close to all paths at once. (b) At the start of the route, the source node delivers the binary strings to the relays located at separate corners by first receiving a random key. This way no eavesdropper close to the source node can obtain all keys (hence cannot decode all binary strings). At the end of the route, the destination combines the binary strings to extract the message (not shown).

5 Conclusions and Future Directions

We have considered the challenges of providing information-theoretic security in a wireless environment, where an eavesdropper near the transmitter of unknown position can make it difficult to choose a rate. Further, the randomness due to the fading, although exploitable if known, makes it impossible to guarantee security performance on slow (block) fading channel. This motivates considering radically different methods to achieve security, and we have considered two recent approaches: one at the physical layer and one at the network layer.

There are still significant challenges to be overcome before information-theoretic security can be reliably employed in wireless networks. In particular the attacker model considered throughout this paper - either a single eavesdropper or non-colluding eavesdroppers - is relatively weak, and many of the schemes are not effective against even mild forms of collusion among the eavesdroppers or active jammers.

References

[1] R. Benson, "The venona story," National Security Agency Central Security Service, Historical Publications (available via WWW).

[2] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction,* Cambridge, 2006.

[3] C. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal,* Vol. 28: pp. 656-715, 1949.

[4] A. Wyner, "The wire-tap channel," *Bell Systems Technical Journal,* Vol. 54: pp. 1355-1387, October 1975.

[5] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory,* Vol. 24: pp. 451-456, July 1978.

[6] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory,* Vol. 39: pp. 733-742, May 1993.

[7] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, I. Secret sharing," *IEEE Transactions on Information Theory,* Vol. 39: pp. 1121-1132, July 1993.

[8] Y. Liang, H. Poor, S. Shamai (Shitz), *Information Theoretic Secrecy,* Now Publishers, 1999.

[9] M. Bloch an J. Barros, *Physical Layer Security: From Information Theory to Security Engineering,* Cambridge, 2011.

[10] A. Shamir, "How to Share a Secret," *Commun. ACM.* Vol. 22: pp. 612-613, November 1979.

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, Vol. 7: pp. 2180-2189, 2008.

[12] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Exploiting the Non-Commutativity of Nonlinear Operators for Information-Theoretic Security in Disadvantaged Wireless Environments," Allerton Conference on Control, Communications, and Computing, October 2012.

[13] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Everlasting Secrecy by Exploiting Non-Idealities of the Eavesdropper's Receiver," *IEEE Journal on Selected Areas in Communications: Special Issue on Signal Processing Techniques for Wireless Physical Layer Security,* Vol. 31: pp. 1828-1839, September 2013.

[14] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Artificial Intersymbol Interference (ISI) to Exploit Receiver Imperfections for Secrecy," IEEE International Symposium on Information Theory (ISIT), July 2013.

[15] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Everlasting Secrecy in Disadvantaged Wireless Environments against Sophisticated Eavesdroppers," submitted to IEEE International Symposium on Information Theory (ISIT), 2014.

[16] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret Communication in Large Wireless Networks without Eavesdropper Location Information," *IEEE InfoCom,* March 2012.

[17] C. Capar and D. Goeckel, "Network Coding for Facilitating Secrecy in Large Wireless Networks," *Proceedings of the Conference on Information Sciences and Systems (CISS)*, March 2012.

[18] D. Goeckel, C. Capar, and D. Towsley, "Physical-Layer Secrecy in Large Multi-Hop Wireless Networks," *Physical-Layer Security in Wireless Communications,* Auerbach Press, CRC Press, October 2013.