Proceedings of the 5th International Symposium on Communications, Control and Signal Processing,
ISCCSP 2012, Rome, Italy, 2-4 May 2012

On interactive secrecy over erasure networks

László Czap
EPFL, Switzerland
Email: laszlo.czap@epfl.ch

Vinod M. Prabhakaran
TIFR, India
Email: vinodmp@tifr.res.in

Suhas Diggavi
UCLA, USA
Email: suhas@ee.ucla.edu

Christina Fragouli
EPFL, Switzerland
Email: christina.fragouli@epfl.ch

***Abstract*—In this short review paper we summarize some of our recent results on interactive message secrecy for broadcast erasure channels.**

I. Introduction

The wireless medium inherently has a broadcast nature. Many recent results demonstrate that when multiple legitimate users share a channel there are significant rate benefits to overhear packets meant for other users [8], [9], [10], [11], [12]. However, to make broadcast transmissions maximally useful for every party, since receivers collect packets meant for other receivers, serious security questions arise. The basic question is whether we can keep messages secret from unintended receivers, while still making use of the broadcast property for transmission efficiency. Also signals can be overheard by anyone with a receiving antenna even if we are attempting to establish a point-to-point link. Therefore the broadcast property makes it easier for a passive eavesdropper to launch an attack against the secrecy of the messages.

Our focus in this paper is on giving information-theoretic security guarantees. The problem of secret communication over a wiretapped channel has been widely investigated since Wyner's seminal paper [1]. It was also observed that a public discussion channel can significantly improve the rate of achievable secret communication [2], [3]. We limit our attention to the case where the public discussion is restricted to the state-feedback the channel. As pointed out in [4] this makes a clear distinction between the *secret key generation* and *secret message sending* problem.

Applying ideas from information theory for wireless network security has been a topic which has attracted significant recent interest (see [13] for a recent survey). The basic property that is used for most information-theoretically secure schemes is to utilize (statistical) *advantages* in the communication links to legitimate nodes over those experienced by the eavesdropper (adversary) nodes. These are exploited to give security against even computationally unbounded adversaries. Since most results focus on giving security guarantees when there is some dimension in which the legitimate receiver's reception is better than the eavesdropper's, a natural question arises on whether we can guarantee such an advantage. A valid criticism is that such advantages which rely on getting the right network conditions cannot be guaranteed to occur naturally; thereby questioning the validity of security guarantees.

In order to address this issue, we made a case in [14] for a different approach where it is possible to *artificially* create an environment, using only dumb interferers, where all nodes in the network experience (statistically) identical but independent communication channels. Though this does occur in several natural (fast fading channel) situations, we cannot guarantee the benevolence of nature, and hence the attempt to enhance nature to create this environment. In [14] we have a preliminary implementation of a wireless security test-bed with such artificial network conditions has been created. For such network conditions, there is no statistical advantage that the legitimate receivers have over the eavesdropper. Then the only mechanism to create secrecy is to use interaction (feedback). To further give flexibility for different types of secrecy guarantees, we use wiretap codes at the physical layer to artificially create independent message-level erasure channels. This not only gives design flexibility, but also enables characterizations for several important special secrecy requirements.

In this paper we summarize some of our progress on the following questions:

- What is the maximal rate at which a common key can be generated between two parties in the presence of an eavesdropper?
- Assuming one sender and one receiver in the presence of an eavesdropper, at what rates can a secret message be conveyed to the receiver?
- Having two or more "honest-but-curious" receivers, how can we simultaneously maintain secrecy and keep transmissions maximally useful?
- How does the secrecy capacity region change if we cannot trust the feedback of the receivers?

Assuming a broadcast erasure channel model, we provide exact characterizations for the above problems. We provide outer bounds for the achievable rates and also simple linear schemes that meet these bounds.

II. Model and notation

A standard point-to-point channel model for wireless communication has been well established as a linear model [15], where the received signal $y_j[t]$ for a node at time t is,

$$y_j[t] = \sum_{i \in \mathcal{N}} h_{ij}[t] x_i[t] + z_j[t], \tag{1}$$

where $\{h_{ij}[t]\}$ represent the channel gains from nodes $\mathcal{N}$ transmitting $\{x_i[t]\}$, and $z_j[t]$ is just receiver (Gaussian) noise, which we will assume to be zero-mean and unit variance

978-1-4673-0276-0/12/$31.00

throughout this paper. This model captures both the superposition and broadcast nature of the wireless channel, since the received signal is the (scaled) sum of all transmitted signals and every transmitted signal affects any receiver. The model (1) equally applies to both legitimate receivers and eavesdroppers. A significant amount of literature on information-theoretic security starts with the model in (1) and develops secure message transmission rates under different assumptions of the channel models.

In our preliminary work [14], we have built a wireless testbed where we place a set of "dumb" antennas in a controlled location (like an auditorium or seminar room), which produce random interfering signals, causing the received signal at any node at the lth time-block of length T symbols to be effectively:

$$y_j^{(l)}[t] = h_{Aj}x_A[t] + \underbrace{\sum_{i\in\mathcal{I}} g_{ij}^{(l)} s_i[t] + z_j[t]}_{\widetilde{z}_j[t]}, t = 1, \ldots, T, \quad (2)$$

where $\{g_{ij}^{(l)}\}$ are independent over blocks indexed by l and independent over receiver nodes j. This implies that different receivers over time experience independent interference which are statistically identically distributed. Since the interfering signals are independent of the information-bearing signal and are essentially random noise, this causes random independent variations of the receiver signal-to-noise ratios (SNR). We emphasize our motivation to create this model is that we do not know the location of the adversary and so we make the channels statistically equivalent (though independent at different locations).

For simplicity[1], we will assume that the interference $\widetilde{z}_j[t]$ have powers that are quantized into S levels, *i.e.,* $\mathbb{E}[|\widetilde{z}_j|^2] \in \{N_1, \ldots, N_S\}$. This results in S different SNRs $\{\frac{P}{N_1}, \ldots, \frac{P}{N_S}\}$. Thus we have a state-dependent channel model, where the SNR depends on the interference state experienced. The probability of the states are determined by the probability of values taken on by interference $\widetilde{z}_j[t]$, which in turn is determined by the induced time variations by the (dumb) interferers.

Connecting signal-level wireless channel to erasures: Given the channel conditioning described in (2), we can create physical layer coding schemes to create secrecy. However, we additionally ask our transmitters to create message-level erasure channels using physical layer (nested) wiretap codes. The mechanism to convert the channel variations into erasure channels using a wiretap code for the the S-state channel is illustrated in Figure 1. Figure $1(a)$ illustrates a wiretap code using a linear deterministic approximation model [16], how we can use channel SNR as a mechanism to obscure transmitted bits. Therefore we can transmit secret messages to a stronger receiver while effectively "erasing" them from the weaker receiver. Having multiple levels of signal strength will then correspond to multiple messages with a nested structure being erased (see Figure 1).

Separation architecture: The approach illustrated in Figure 1 is really a separation architecture for secrecy. In particular using the channel conditioning of (2), we design the physical layer (nested) wiretap code to create (multiple-level) erasure channels, independent and identically distributed for users. Then, as seen in the review of results in Section III, we can design interactive secrecy strategies for such erasure networks. We advocate such an architecture since it enables two things. One is flexibility, *i.e.,* the physical layer becomes oblivious to different security requirements; for example the same physical layer can be used to generate secure keys as well as message security, as seen in the results of Section III. Moreover, since the interface is a simple erasure channel, efficient and scalable (linear) secrecy strategies can be implemented. This modular approach has a basis in the layered IP network architecture which made the Internet successful. By perhaps slightly sacrificing the amount of secrecy (if the physical layer is more intricately designed for particular secrecy needs) we get benefits in complexity and flexibility[2]. Therefore for S-message levels $\{W_1, \ldots, W_S\}$, the separation-based effectively gives a message-level erasure model, where the observation $\mathcal{T}_i$ for receiver i in state s given by:

$$\mathcal{T}_i = \{W_1, \ldots, W_l, ?, \ldots, ?\} \text{ if state } s = l, \quad (3)$$

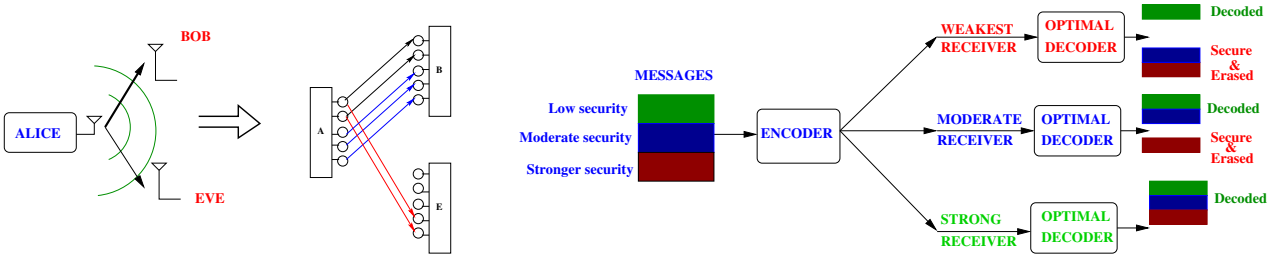
where ? implies "erasure" *i.e.,* the messages $\{W_{l+1}, \ldots, W_S\}$ are completely secret from receiver in state l. The erasure probabilities are influenced the the probability of the state-dependent model of (2) and the rates of nested messages determined by the nested wiretap codes.

For simplicity we will focus on $S = 2$ states, with the understanding that these techniques can be generalized to arbitrary number of message-level erasure states. This implies that for the purposes of this paper, communication takes place over a 1-to-K broadcast erasure channel. The input alphabet of the channel consists of all possible vectors of length L over a finite field $\mathbb{F}_q$. For convenience, we usually call each such vector a *packet*. We denote by X_i the ith transmission over the channel, and by $Y_{1,i}, Y_{2,i}, Y_{3,i}$ the corresponding outputs observed by the receivers. We use X^n to denote the vector $(X_1, X_2, \ldots, X_n)$ and similarly for other vectors also. The broadcast channel is made up of independent component erasure channels with erasure probabilities $\delta_1, \ldots, \delta_K$:

$$\Pr\{Y_{1,i}, \ldots, Y_{K,i}|X_i\} = \prod_{j=1}^{K} \Pr\{Y_{j,i}|X_i\}$$

[1]In principle we can extend this to arbitrary fine quantization, though its utility will only go up to noise power (which is assumed to be 1).

[2]Though there might be some gain by not restricting ourselves to the separation architecture, in this paper, we focus on such an approach. Our belief is that the gains are small, since what we ignore are learning the receiver noises and we focus more on the interference variations which are much larger. Many ideas of wireless secrecy based on reciprocity of wireless channels have been proposed [18], [20], [21], [19]. The secrecy rates obtained by such schemes are much lower than our scheme [14] and ensuring the channel independence without conditioning the network makes the secrecy guarantees more vulnerable to criticism.



(a) Signal-level model

(b) Message-level erasures

Figure 1. Figure (a): Illustration of connection between signal-level wireless channel and erasures using the deterministic model for broadcast. Channel from Alice to Bob (and Eve) has two states of SNR approximately 15dB and approximately 6dB. This translates to 5 bits and 2 bits for each state (capacity of $\log(1+\text{SNR})$ translates to roughly 1 bit per 3dB). This is modeled deterministically on the right (see [16] for more details). Therefore if either Bob or Eve are in the worse state only 2 bits of Alice's transmission are "visible" to either of them and we can keep 3 bits secret from this state through layered secure coding for Gaussian channels [17]. Note that *both* Bob and Eve have independent and identically distributed state sequences and therefore without feedback/interaction there can be no secrecy. Figure (b): If there are potentially multiple levels of channel SNR that all receivers and eavesdroppers can see, then we can extend the ideas from Figure $1(a)$ to multiple levels of secure messages. For example, if all the receivers (including eavesdropper) can have 3 channel SNRs, then we can encode such that only the most insecure message is "visible" at the lowest channel SNR; only the two lowest messages are visible at moderate SNR and so on. This creates a erasure channel at every message level, with different erasure probabilities.

$$\forall j \in \{1,\ldots,K\} : \Pr\{Y_{j,i}|X_i\} = \begin{cases} 1-\delta_j, & Y_{j,i} = X_i \\ \delta_j, & Y_j = \perp, \end{cases}$$

where $\perp$ is the symbol of an erasure.

Further, we assume that the (erasure) state S_i of the channel during the ith transmission (i.e., which receivers experienced erasures) is strictly causally available to all parties. The only exception is when one of the parties is a passive eavesdropper, in which case we assume that the state of the eavesdropper's channel is not part of S_i. To make the distinction, we denote by Z^n the eavesdropper's output and by δ_E the corresponding erasure probability.

III. Review of results

1) One receiver: First, let us assume a single unicast session in the presence of a passive eavesdropper [5], [4].

Theorem 1. *The secret key generation capacity of the broadcast erasure channel with state-feedback is*

$$C_{SK} = \delta_E(1-\delta_1)L\log q. \tag{4}$$

Theorem 2. *The secret message sending capacity of the broadcast erasure channel with state-feedback is*

$$C_{SM} = \delta_E(1-\delta_1)\frac{1-\delta_1\delta_E}{1-\delta_1\delta_E^2}L\log q. \tag{5}$$

2) Two receivers: Consider a broadcast channel with two receivers where the sender wants to send independent private messages each of the receivers; there are no eavesdroppers. The secrecy requirement is that neither receiver must learn any information about the message meant for other receiver. We have the following result [6]:

Theorem 3. *The secret message capacity region is the set of all rate pairs $(R_1,R_2) \in \mathbb{R}_+^2$ which satisfy the following two inequalities:*

$$\frac{R_1(1-\delta_2)}{\delta_2(1-\delta_1)(1-\delta_1\delta_2)} + \frac{R_1}{1-\delta_1} + \frac{R_2}{1-\delta_1\delta_2} \le L\log q, \tag{6}$$

$$\frac{R_2(1-\delta_1)}{\delta_1(1-\delta_2)(1-\delta_1\delta_2)} + \frac{R_1}{1-\delta_1\delta_2} + \frac{R_2}{1-\delta_2} \le L\log q. \tag{7}$$

This capacity region remains unchanged irrespective of whether the users are honest-but-curious or malicious. See [6] for precise defintions of these security notions in this context.

Related to the theme of the paper, we also have results on group key generation both for erasure channels [5], [14] as well as deterministic channels and Gaussian networks [7].

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell system Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channels," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 2437–2452, 2008.

[4] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. Diggavi, "Secret message capacity of erasure broadcast channels with feedback," in *Information Theory Workshop (ITW)*, 2011, pp. 65–69.

[5] M. Jafari Siavoshani, S. Diggavi, C. Fragouli, U. K. Pulleti, and K. Argyraki, "Group secret key generation over broadcast erasure channels," in *Asilomar Conference on Signals, Systems, and Computers*, 2010, pp. 719–723.

[6] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. Diggavi, "Secure capacity region for erasure broadcast channels with feedback," ArXiv, abs/110.5741, 2011. [Online]. Available: http://http://arxiv.org/abs/1110.5741

[7] M. Jafari Siavoshani, S. Mishra, S N. Diggavi and C. Fragouli, *Group secret key agreement over state-dependent wireless broadcast channels*. IEEE International Symposium on Information Theory (ISIT), August 2011.

[8] Wu, Y., Chou, P., Kung, S.: Information exchange in wireless networks with network coding and physical-layer broadcast. In: Conference on Information Sciences and Systems (CISS). (2005)

[9] Georgiadis, L., Tassiulas, L.: Broadcast erasure channel with feedback-capacity and algorithms. In: Workshop on Network Coding, Theory, and Applications, (NetCod), IEEE (2009) 54–61

[10] Maddah-Ali, M., Tse, D.: Completely stale transmitter channel state information is still very useful. In: 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton). (2010) 1188–1195

[11] Gatzianas, M., Georgiadis, L., Tassiulas, L.: Multiuser broadcast erasure channel with feedback - capacity and algorithms. ArXiv, abs/1009.1254 (2010)
[12] Dana, A.F., Hassibi, B.: The capacity region of multiple input erasure broadcast channels. In: International Symposium on Information Theory (ISIT). (2005) 2315–2319
[13] Y. Liang, H V. Poor, and S. Shamai. *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory, 2009.
[14] M. Jafari Siavoshani, U. Pulleti, E. Atsan, I. Safaka, C. Fragouli, K. Argyraki, S. Diggavi. *Exchanging Secrets without Using Cryptography*. http://arxiv.org/abs/1105.4991, 2011.
[15] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, May 2005.
[16] S. Avestimehr, S N. Diggavi and D. Tse, "Wireless network information flow: a deterministic approach", vol 57, number 4, pp 1872–1905, *IEEE Transactions on Information Theory*, April 2011.
[17] Y. Liang, L. Lai, H. V. Poor, and S. Shamai (Shitz), "The Broadcast Approach over Fading Gaussian Wiretap Channels," *IEEE Information Theory Workshop*, 2009.
[18] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Communications Letters*, vol. 4, no. 2, pp. 52-55, Feb. 2000.
[19] J. Croft, N. Patwari, and S. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *ACM IPSN*, Sweden, Apr. 2010.
[20] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364-375, Sep. 2007.
[21] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240-254, Jun. 2010.