Capacity Results on the Finite State Markov Wiretap Channel with Delayed State Feedback

Bin Dai*†, Zheng Ma*
* School of Information Science and Technology, Southwest JiaoTong University, Chengdu 610031, China,
Email: daibin@home.swjtu.edu.cn, zma@home.swjtu.edu.cn.
† The State Key Laboratory of Integrated Services Networks, Xidian University, Xi′an, Shaanxi 710071, China.

***Abstract*—The finite state Markov channel (FSMC) has been shown to be a useful model for the time-varying fading channels. In this paper, we study the security issue in the wireless communication systems by considering the FSMC with an eavesdropper, which we call the finite state Markov wiretap channel (FSM-WC). More specifically, the FSM-WC is a channel with one input (the transmitter) and two outputs (the legitimate receiver and the eavesdropper). The transition probability of the FSM-WC is controlled by a channel state which takes values in a finite set, and it undergoes a Markov process. We assume that the state is perfectly known by the legitimate receiver and the eavesdropper, and through a noiseless feedback channel, the legitimate receiver sends the state back to the transmitter after some time delay. Measuring the eavesdropper's uncertainty about the transmitted message by equivocation, we provide inner and outer bounds on the capacity-equivocation region of this novel model, and show that these bounds meet (the capacity-equivocation region is determined) if the channel output for the eavesdropper is a degraded version of that for the legitimate receiver. The capacity results of this paper are further explained via degraded Gaussian and Gaussian fading examples.**

***Index Terms*—Capacity-equivocation region, delayed state feedback, finite-state Markov channel, secrecy capacity, wiretap channel.**

I. Introduction

The finite state Markov channel (FSMC) is a discrete channel whose transition probability is controlled by a state which takes values in a finite set, and the state undergoes a Markov process. Wang et al. [1] and Zhang et al. [2] found that the FSMC was a useful model for the time-varying fading channels, and the capacity of the FSMC was studied by [3]. In practical mobile wireless communication systems, the channel state is usually obtained by the transmitter via the receiver's feedback, and this feedback is often not instantaneous, i.e., the transmitter often receives delayed state from the receiver. This communication scenario can be modeled as the finite state Markov channel with delayed feedback, see Figure 1. The model of Figure 1 was investigated by Viswanathan [4], and the capacity of this channel model was totally determined. Moreover, Viswanathan [4] pointed out that the delayed receiver's channel output feedback does not increase the capacity of the model of Figure 1, i.e., there is no need for the receiver to send his channel output back to the transmitter at each time instant. Other related works on the FSMC are in [5]-[10].

Wyner's work on wiretap channel [11] and Csiszár-Körner's work on the broadcast channel with confidential messages [12] lay the foundation of the information-theoretic security in communication systems. Using the approach of [11] and [12], the security problems in multi-user communication channels, such as broadcast channel, multiple-access channel, relay channel, and interference channel, have been widely studied, see [13]-[28]. Recently, Wyner's wiretap channel with states has received much attention, see [29]-[32]. These works focus on the scenario that the states are identical independent distributed (i.i.d.), and to the best of the authors' knowledge, only Bloch et al. [33] and Sankarasubramaniam et al. [34] investigated the wiretap channel with memory states, where a stochastic algorithm for computing the multi-letter form secrecy capacity of this model was provided. A single-letter characterization for the secrecy capacity of [33] and [34] is still open.

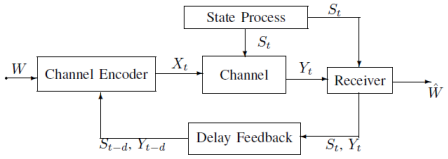

Fig. 1: The FSMC with delayed feedback

In this paper, we investigate the information-theoretic security in wireless communication networks by combining Wyner's wiretap channel model with the model of Figure 1, see Figure 2. In Figure 2, the transition probability of the channel at each time instant depends on a state which undergoes a finite-state Markov process. At time i, the receiver (**throughout this paper, the "receiver" is used as a shorthand for "legitimate receiver"**) receives the state S_i, and sends it back to the transmitter after a delay time d via a noiseless feedback channel. The channel encoder, at time i, generates the channel input according to the transmitted message W and the delayed state feedback S_{i-d}. Moreover, at time i, we assume that a powerful eavesdropper also receives the state S_i, and he wishes to obtain the transmitted message W. The delay time d is perfectly known by the receiver, the eavesdropper and the transmitter. Inner and outer bounds on the capacity-equivocation region of the model of Figure 2 are provided in this paper, and we show that these bounds meet if the channel output for the eavesdropper is a degraded

version of that for the legitimate receiver. These capacity results are further explained via a degraded Gaussian example. The rest of this paper is organized as follows. In Section II,

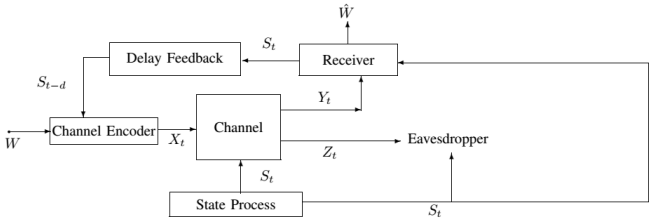

Fig. 2: The FSM-WC with delayed state feedback

we show the definitions and the main results of the model of Figure 2. Degraded Gaussian and Gaussian fading examples of the model of Figure 2 are provided in Section III. Final conclusions and future works are presented in Section IV. In the remainder of this paper, the log function is taken to the base 2.

II. Definitions and the Main Result of the Model of Figure 2

The channel is a finite-state Markov channel (FSMC), where the channel state S takes values in a finite alphabet $\mathcal{S} = \{s_1, s_2, ..., s_k\}$. At the i-th time ($1 \le i \le N$), the channel outputs Y_i and Z_i depend only on X_i and S_i, and thus the channel transition probability $P_{Y^N,Z^N|X^N,S^N}(y^N, z^N|x^N, s^N) = \prod_{i=1}^{N} P_{Y,Z|X,S}(y_i, z_i|x_i, s_i)$. The state process $\{S_i\}$ is assumed to be a stationary irreducible aperiodic ergodic Markov chain, and it is independent of the transmitted messages. Furthermore, it satisfies

$$\begin{aligned} &Pr\{S_i = s_i|X^i = x^i, Y^i = y^i, S^{i-d} = s^{i-d}\} \\ &= Pr\{S_i = s_i|S_{i-d} = s_{i-d}\}, \end{aligned} \tag{2.1}$$

where $1 \le d \le i-1$. Denote the 1-step transition probability matrix by K, and denote the steady state probability of $\{S_i\}$ by π. Let the random variables S_i and S_{i-d} be the channel states at time i and $i-d$, respectively. The joint distribution of (S_i, S_{i-d}) is given by

$$\pi_d(S_i = s_l, S_{i-d} = s_j) = \pi(s_j)K^d(s_j, s_l), \tag{2.2}$$

where s_l is the l-th element of $\mathcal{S}$, s_j is the j-th element of $\mathcal{S}$, and $K^d(s_j, s_l)$ is the (j,l)-th element of the d-step transition probability matrix K^d of the Markov process..

Let W, uniformly distributed over the alphabet $\mathcal{W} = \{1, 2, ..., M\}$, be the message sent by the transmitter. The i-th time channel input X_i is given by

$$X_i = \begin{cases} f_i(W), & 1 \le i \le d \\ f_i(W, S^{i-d}), & d+1 \le i \le N. \end{cases} \tag{2.3}$$

Here note that the i-th time channel encoder f_i is a stochastic encoder. The channel decoder is a mapping

$$\psi: \ \mathcal{Y}^N \times \mathcal{S}^N \to \{1, 2, ..., M\}, \tag{2.4}$$

with inputs Y^N and S^N and output $\hat{W}$. The average probability of error P_e is denoted by

$$P_e = \frac{1}{M}\sum_{i=1}^{M}\sum_{s^N} P_{S^N}(s^n) Pr\{\psi(y^N, s^N) \ne i | i \text{ was sent}\}. \tag{2.5}$$

Since the state is also known by the eavesdropper, the eavesdropper's equivocation to the message W is defined as

$$\Delta = \frac{1}{N} H(W|Z^N, S^N). \tag{2.6}$$

A rate pair (R, R_e) (where $R, R_e > 0$) is called achievable if, for any $\epsilon > 0$, there exists a channel encoder-decoder (N, Δ, P_e) such that

$$\frac{\log M}{N} \ge R - \epsilon, \ \Delta \ge R_e - \epsilon, \ P_e \le \epsilon. \tag{2.7}$$

The capacity-equivocation region of the model of Figure 2 is a set composed of all achievable (R, R_e) pairs, and it is denoted by $\mathcal{R}$.

Main results on $\mathcal{R}$:

Theorem 1: An inner bound $\mathcal{R}^{in}$ on $\mathcal{R}$ is given by

$$\begin{aligned} \mathcal{R}^{in} = \{&(R, R_e): 0 \le R_e \le R, \\ &R \le I(V; Y|S, \tilde{S}), \\ &R_e \le I(V; Y|U, S, \tilde{S}) - I(V; Z|U, S, \tilde{S})\}, \end{aligned}$$

where the joint probability $P_{UVS\tilde{S}XYZ}(u, v, s, \tilde{s}, x, y, z)$ satisfies

$$\begin{aligned} &P_{UVS\tilde{S}XYZ}(u, v, s, \tilde{s}, x, y, z) \\ &= P_{YZ|XS}(y, z|x, s) P_{X|UV\tilde{S}}(x|u, v, \tilde{s}) P_{V|U\tilde{S}}(v|u, \tilde{s}) \cdot \\ &P_{U|\tilde{S}}(u|\tilde{s}) K^d(\tilde{s}, s) P_{\tilde{S}}(\tilde{s}), \end{aligned}$$

$K^d(\tilde{s}, s) = P_{S|\tilde{S}}(s|\tilde{s})$, and U may be assumed to be a (deterministic) function of V.

Proof: The message W is split into a common message represented by the auxiliary random variable U and a confidential message represented by the auxiliary random variable V. The delayed feedback state S_{i-d} is represented by the auxiliary random variable $\tilde{S}$. Theorem 1 is proved by using a multiplexing random binning coding scheme, which combines Wyner's random binning technique [11] with the multiplexing coding for the finite state Markov channel (FSMC) with delayed state feedback [4]. The details of the proof of Theorem 1 are in [37, pp. 17-24]. ■

Theorem 2: An outer bound $\mathcal{R}^{out}$ on $\mathcal{R}$ is given by

$$\begin{aligned} \mathcal{R}^{out} = \{&(R, R_e): 0 \le R_e \le R, \\ &R \le I(V; Y|S, \tilde{S}), \\ &R_e \le I(V; Y|U, S, \tilde{S}) - I(V; Z|U, S, \tilde{S})\}, \end{aligned}$$

where the joint probability $P_{UVS\tilde{S}XYZ}(u, v, s, \tilde{s}, x, y, z)$ satisfies

$$\begin{aligned} &P_{UVS\tilde{S}XYZ}(u, v, s, \tilde{s}, x, y, z) \\ &= P_{YZ|XS}(y, z|x, s) P_{XVUS\tilde{S}}(x, v, u, s, \tilde{s}). \end{aligned}$$

Proof: Theorem 2 is proved by introducing the delayed feedback state S_{i-d} into the converse proof of the broadcast channel with confidential messages [12], and defining the following auxiliary random variables

$$U \triangleq (Y^{J-1}, Z_{J+1}^N, S^N, J), V \triangleq (U, W),$$
$$S \triangleq S_J, \tilde{S} \triangleq S_{J-d}, Y \triangleq Y_J, Z \triangleq Z_J, \quad (2.8)$$

where J is a random variable uniformly distributed over $\{1, 2, , ..., N\}$, and it is independent of Y^N, Z^N, W and S^N. Due to the limits of the paper length, we omit the proof here, and the details are in [37, pp. 24-27]. ■

Remark 1: There are some notes on Theorem 1 and Theorem 2, see the followings.

- Here note that the inner bound $\mathcal{R}^{in}$ is almost the same as the outer bound $\mathcal{R}^{out}$, except the definitions of the joint probability $P_{UVS\tilde{S}XYZ}(u, v, s, \tilde{s}, x, y, z)$ in $\mathcal{R}^{in}$ and $\mathcal{R}^{out}$. To be specific, in $\mathcal{R}^{in}$, the definition of $P_{UVS\tilde{S}XYZ}(u, v, s, \tilde{s}, x, y, z)$ implies the Markov chains $S \to (S, U, V) \to X$, $S \to (\tilde{S}, U) \to V$ and $S \to \tilde{S} \to U$, but these chains are not guaranteed in $\mathcal{R}^{out}$.
- If the eavesdropper's received symbol Z^N is a degraded version of Y^N, i.e., the Markov chain $(X^N, S^N) \to Y^N \to Z^N$ holds, the outer bound $\mathcal{R}^{out}$ meets with the inner bound $\mathcal{R}^{in}$, and they reduce to the following region $\mathcal{R}^*$, where

$$\mathcal{R}^* = \{(R, R_e) : R_e \le R,$$
$$R \le I(X; Y|S, \tilde{S}),$$
$$R_e \le I(X; Y|S, \tilde{S}) - I(X; Z|S, \tilde{S})\}. \quad (2.9)$$

Proof: See [37, pp. 27-30]. ■

III. Examples

A. Secrecy Capacity for the Degraded Gaussian Case of the model of Figure 2

For the degraded Gaussian case of Figure 2, at the i-th time ($1 \le i \le N$), the inputs and outputs of the channel satisfy

$$Y_i = X_i + N_{S_i}, \ Z_i = Y_i + N_{w,i}. \quad (3.1)$$

Here note that N_{S_i} is Gaussian distributed with zero mean, and the variance of N_{S_i} depends on the i-th time state $S_i = s_i$ (denoted by $\sigma_{s_i}^2$). The random variable $N_{w,i}$ ($1 \le i \le N$) is also Gaussian distributed with zero mean and constant variance σ_w^2. The power constraint of the transmitter is given by $\sum_{\tilde{s}} \pi(\tilde{s}) E_{P_{X|\tilde{S}}(x|\tilde{s})}[X^2|\tilde{s}] \le \mathcal{P}_0$. The secrecy capacity $\mathcal{C}_s$ of the degraded case of Figure 2 can be directly obtained from $\mathcal{R}^*$ by letting $R_e = R$ and maximizing R. Using the degradedness assumption and the entropy power inequality, it is not difficult to calculate the secrecy capacity C_s^g of the degraded Gaussian case of Figure 2, and it is given by

$$C_s^g = \max_{\mathcal{P}(\tilde{s}): \sum_{\tilde{s}} \pi(\tilde{s}) \mathcal{P}(\tilde{s}) \le \mathcal{P}_0} \sum_{\tilde{s}} \sum_{s} \pi(\tilde{s}) K^d(\tilde{s}, s)$$
$$(\frac{1}{2} \log(1 + \frac{\mathcal{P}(\tilde{s})}{\sigma_s^2}) - \frac{1}{2} \log(1 + \frac{\mathcal{P}(\tilde{s})}{\sigma_s^2 + \sigma_w^2})), \quad (3.2)$$

where $\mathcal{P}(\tilde{s})$ is the transmitter's power for the state $\tilde{s}$, and σ_s^2 is the variance of the noise N_S given the state $S = s$. These definitions are similar to those in [4, pp. 764-765], and the details of the proof of (3.2) are in [37, pp. 9-10]. In order to gain some intuition on the secrecy capacity of (3.2), we consider a simple case that the state alphabet $\mathcal{S}$ is composed of only two elements. At each time instant, the state of the channel is G (good state) or B (bad state). For the state G (B), the noise variance of the channel is σ_G^2 (σ_B^2). Here note that $\sigma_B^2 > \sigma_G^2$. The state process is given by

$$P(G|G) = 1 - b, P(B|G) = b, P(B|B) = 1 - g, P(G|B) = g.$$

The steady state probabilities $\pi(G)$ and $\pi(B)$ are given by

$$\pi(G) = \frac{g}{g + b}, \ \pi(B) = \frac{b}{g + b}. \quad (3.3)$$

Define $u = 1 - g - b$ and $c = g/b$. The parameter u is related to the channel memory (Mushkin and Bar-David [35] has already shown that the channel memory is increasing while u is increasing), and the parameter c controls the steady state distributions (see 3.3). Fixing c (for example, $c = 1$), we can choose different u, d and σ_w^2 to investigate the effects of channel memory, feedback delay and the eavesdropper's channel noise variance on the secrecy capacity C_s^g. As we can see in Figure 3, when the channel is changing rapidly (which implies that the channel memory u is small, for example, $u = 0.02$), the secrecy capacity goes to the infinite asymptote even if $d = 1$. However, when the channel is changing slowly (which implies that the channel memory u is large, for example, $u = 0.9$), a larger feedback delay is tolerable since the secrecy capacity loss compared with feedback without delay ($d = 0$) is smaller. Moreover, it is easy to see that the worse eavesdropper's channel, the larger secrecy capacity.

B. Secrecy Capacity for the Degraded Gaussian Fading Case of the model of Figure 2

For the degraded Gaussian fading case of Figure 2, at the i-th time ($1 \le i \le N$), the channel inputs and outputs satisfy

$$Y_i = g(s_i) X_i + N_{S_i}, \ Z_i = l_i Y_i + N_{w,i}. \quad (3.4)$$

Here $g(s_i)$ is the fading process of the transmitter, and we assume that it is a deterministic function of s_i. The noise N_{S_i} is Gaussian distributed with zero mean, and the variance depends on the i-th time state S_i of the channel. For the eavesdropper, the fading coefficient l_i is a constant, i.e., $l_i = l$ for all $i \in \{1, 2, ..., N\}$. The random variable $N_{w,i}$ ($1 \le i \le N$) is also Gaussian distributed with zero mean and constant variance σ_w^2 ($N_{w,i} \sim \mathcal{N}(0, \sigma_w^2)$ for all $i \in \{1, 2, ..., N\}$). The secrecy capacity C_s^{g*} of the degraded Gaussian fading case of Figure 2 is given by

$$C_s^{(g*)} = \max_{\mathcal{P}(\tilde{s}): \sum_{\tilde{s}} \pi(\tilde{s}) \mathcal{P}(\tilde{s}) \le \mathcal{P}_0} \frac{1}{2} \sum_{\tilde{s}} \sum_{s} \pi(\tilde{s}) K^d(\tilde{s}, s)$$
$$(\frac{1}{2} \log(1 + \frac{g^2(s) \mathcal{P}(\tilde{s})}{\sigma_s^2}) - \frac{1}{2} \log(1 + \frac{g^2(s) l^2 \mathcal{P}(\tilde{s})}{l^2 \sigma_s^2 + \sigma_w^2})). \quad (3.5)$$

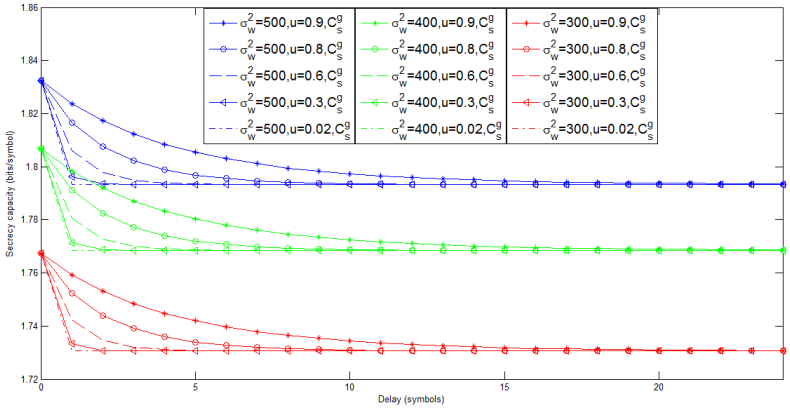

Fig. 3: The secrecy capacity $C_s^{(g)}$ for $\mathcal{P}_0 = 100$, $\sigma_G^2 = 1$, $\sigma_B^2 = 100$, $c = 1$ and several values of u and σ_w^2

Here note that replacing X_i by $g(s_i)X_i$, and Y_i by l_iY_i, the achievability proof of (3.5) is along the lines of that of (3.2), and the converse proof of (3.5) is in [37, p. 14].

In order to gain some intuition on the secrecy capacity of (3.5), we consider a simple two-state case where the state process is the same as that in Subsection III-A. Define $g(G) = 1$, $g(B) = 0.5$, $l = 0.8$, $u = 1 - g - b$ and $c = g/b$. In the following Figure 4 and Figure 5, we compare the secrecy capacities of the fading and non-fading cases for $\mathcal{P}_0 = 100$, $\sigma_G^2 = 1$, $\sigma_B^2 = 100$, $c = 1$, $g(G) = 1$, $g(B) = 0.5$, $l = 0.8$ and several values of u and σ_w^2. It is easy to see that $C_s^{(g*)}$ dominates $C_s^{(g)}$ (which implies that the fading may enhance the security of the degraded Gaussian model of Figure 2), and the gap between $C_s^{(g*)}$ and $C_s^{(g)}$ is increasing while σ_w^2 is decreasing.

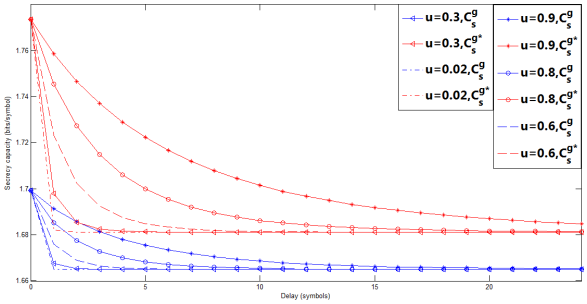

Fig. 4: The comparison of the secrecy capacities $C_s^{(g*)}$ and $C_s^{(g)}$ for $\mathcal{P}_0 = 100$, $\sigma_G^2 = 1$, $\sigma_B^2 = 100$, $\sigma_w^2 = 200$, $c = 1$, $g(G) = 1$, $g(B) = 0.5$, $l = 0.8$ and several values of u

IV. Conclusion

In this paper, we study the FSM-WC with delayed state feedback. Inner and outer bounds on the capacity-equivocation region of this model are provided, and we show that these bounds meet if the channel output for the eavesdropper is a degraded version of that for the legitimate receiver. These bounds are further explained via degraded Gaussian and Gaussian fading examples. Numerical results of these examples show that the secrecy capacity is decreasing while the feedback delay is increasing, the larger channel memory (the channel changes more slowly) leads to a more rapidly decreasing of the secrecy capacity, and the fading may enhance the secrecy capacity of the degraded Gaussian FSM-WC with delayed state feedback. Moreover, note that similar to the well known fact that the output Y^N feedback enhances the capacity-equivocation region of Wyner's wiretap channel (see [36]), in our full paper [37], we show that the receiver's delayed output feedback (Y^N is also fed back to the transmitter after some time delay) also enhances the capacity-equivocation region of the model of this paper.

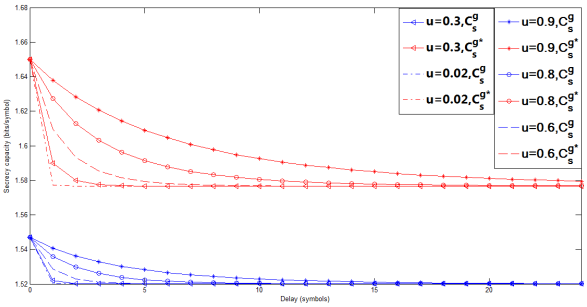

Fig. 5: The comparison of the secrecy capacities $C_s^{(g*)}$ and $C_s^{(g)}$ for $\mathcal{P}_0 = 100$, $\sigma_G^2 = 1$, $\sigma_B^2 = 100$, $\sigma_w^2 = 100$, $c = 1$, $g(G) = 1$, $g(B) = 0.5$, $l = 0.8$ and several values of u

Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grants 61671391, 61301121 and 61571373, the fundamental research funds for the Central universities (No. 2682016ZDPY06), and the Open Research Fund of the State Key Laboratory of Integrated Services Networks, Xidian University (No. ISN17-13).

REFERENCES

[1] H. S. Wang and N. Moayeri, "Finite-state markov channel-A useful model for radio communication channels," *IEEE Trans. Veh. Technol*, vol. 44, pp. 163-171, 1995.

[2] Q. Zhang and S. Kassam, "Finite-state Markov model for Rayleigh fading channels," *IEEE Trans. Commun*, vol. 47, no. 11, pp. 1688-1692, 1999.

[3] A. J. Goldsmith and P. P. Varaiya, "Capacity, mutual information, and coding for finite-state Markov channels," *IEEE Trans. Inf. Theory*, vol. IT-42, pp. 868-886, 1996.

[4] H. Viswanathan, "Capacity of Markov channels with receiver CSI and delayed feedback," *IEEE Trans. Inf. Theory*, vol. IT-45, no. 2, pp. 761-771, 1999.

[5] U. Basher, A. Shirazi and H. H. Permuter, "Capacity region of finite state multiple-access channels with delayed state information at the Transmitters," *IEEE Trans. Inf. Theory*, vol. IT-58, no. 6, pp. 3430-3452, 2012.

[6] J. Chen and T. Berger, "The capacity of finite-state Markov channels with feedback," *IEEE Trans. Inf. Theory*, vol. IT-51, pp. 780-789, 2005.

[7] H. H. Permuter and T. Weissman, "Capacity region of the finite-state multiple access channel with and without feedback," *IEEE Trans. Inf. Theory*, vol. IT-55, no. 6, 2009.

[8] H. H. Permuter, T. Weissman, and A. J. Goldsmith, "Finite state channels with time-invariant deterministic feedback," *IEEE Trans. Inf. Theory*, vol. IT-55, pp. 644-662, 2009.

[9] G. Como and S. Yüksel, "On the capacity of finite state multiple access channels with asymmetric partial state feedback," in *WiOPT09: Proc. 7th Int. Conf.Modeling and Optimization inMobile, Ad Hoc, and Wireless Networks, IEEE Press*, Piscataway, NJ, 2009, pp. 589-594.

[10] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Trans. Inf. Theory*, vol. IT-43, pp. 1986-1992, 1997.

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

[12] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[13] R. Liu, I. Maric, P. Spasojevic and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 6, pp. 2493-2507, Jun. 2008.

[14] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-55, no. 6, pp. 4529-4542. 2009.

[15] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 3, pp. 976-1002, Mar. 2008.

[16] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 12, pp. 5747-5755, Dec. 2008.

[17] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 6, pp. 2735-2751, June 2008.

[18] M. Wiese and H. Boche, "An Achievable Region for the Wiretap Multiple-Access Channel with Common Message," *Proceedings of 2012 IEEE International Symposium on Information Theory*, 2012.

[19] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," *Proceedings of IEEE Information Theory Workshop*, 2010.

[20] P. Xu, Z. Ding, and X. Dai, "Rate Regions for Multiple Access Channel With Conference and Secrecy Constraints," *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 12, pp. 1961-1974, 2013.

[21] Z. H. Awan, A. Zaidi and L. Vandendorpe, "Multi-access Channel with Partially Cooperating Encoders and Security Constraints," *IEEE Trans. Inf. Forensics and Security*, Vol. 8, No. 7, pp. 1243-1254, Jul. 2013.

[22] X. Tang, R. Liu, P. Spasojević and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. IT-57, no. 5, pp. 3153-3167, May 2011.

[23] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. IT-55, pp. 604-619, 2009.

[24] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 9, pp. 4005-4019, Sep. 2008.

[25] B. Dai and Z. Ma, "Multiple-access relay wiretap channel," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 9, pp. 1835-1849, Sep. 2015.

[26] Y. Oohama, "Coding for relay channels with confidential messages," in *Proceedings of IEEE Information Theory Workshop*, Australia, 2001.

[27] B. Dai, L. Yu and Z. Ma, "Relay broadcast channel with confidential messages," *IEEE Trans. Inf. Forensics and Security*, vol. 11, no. 2, pp. 410-425, 2016.

[28] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-57, pp. 137-155, 2011.

[29] C. Mitrpant, A. J. Han Vinck and Y. Luo, "An Achievable Region for the Gaussian Wiretap Channel with Side Information," *IEEE Trans. Inf. Theory*, vol. IT-52, no. 5, pp. 2181-2190, 2006.

[30] Y. Chen, A. J. Han Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 1, pp. 395-402, January 2008.

[31] B. Dai, Z. Ma and X. Fang, "Feedback Enhances the Security of State-Dependent Degraded Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Forensics and Security*, Vol. 10, No. 7, pp. 1529-1542, 2015.

[32] Y. K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2838-2849, May 2012.

[33] M. Bloch and J. N. Lanema, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. of 46th Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

[34] Y. Sankarasubramaniam, A. Thangaraj and K. Viswanathan, "Finite-state wiretap channels: secrecy under memory constraints," in *Proc. 2009 IEEE Information Theory Workshop*, Taormina, Italy, 2009, pp. 115-119.

[35] M. Mushkin and I. Bar-David, "Capacity and coding for the Gilbert-Elliott channels," *IEEE Trans. Inf. Theory*, vol. 35, pp. 1277-1290, 1989.

[36] R. Ahlswede and N. Cai, "Transmission, Identification and Common Randomness Capacities for Wire-Tap Channels with Secure Feedback from the Decoder," book chapter in *General Theory of Information Transfer and Combinatorics*, LNCS 4123, pp. 258-275, Berlin: Springer-Verlag, 2006.

[37] B. Dai, Z. Ma and Y. Luo, "Finite State Markov Wiretap Channel with Delayed Feedback," http://arxiv.org/abs/1606.06418.