

A Secure Method for Transmission of Sensitive Data over Wireless Fading Channels

B. Kavitha¹, K. S. Yuvaraj²

¹PG Scholar, Department of MCA, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

²Ass. Professor, Department of MCA, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

ABSTRACT

In this project, the Delay-Sensitive data capacity of the Wireless fading channel is explored under two distinct suppositions on the accessible transmitter channel state data (CSI). The principal situation accept consummate earlier learning of both the fundamental and spy channel picks up. Here, upper and lower limits on the protected delay constrained limit are inferred and appeared to be tight in the high flag to-clamor proportion (SNR) administration (for a wide class of channel circulations). In the second situation, just the principle channel CSI is thought to be accessible at the transmitter. Amazingly, under this suspicion, I build up the achievability of non-zero secure rate (for a wide class of channel circulations) under a strict delay limitation. In the two cases, our achievability contentions depend on a novel two phase approach that defeats the mystery blackout wonder saw in before works.

Keywords : Delay-Sensitive Data Capacity, Wireless Fading, Channel State Data, Secure Method, Quality of Service, SNR

I. INTRODUCTION

In many applications, there is a delay constraint on the data to be transmitted via a wireless link. These applications range from the most basic voice communication to the more demanding multimedia streaming. However, due to its broadcast nature, the wireless channel is vulnerable to eavesdropping and other security threats. Therefore, it is of critical importance to find techniques to combat these security attacks while satisfying the delay limitation imposed by the Quality of Service (QoS) constraints. This motivates our analysis of the fundamental information theoretic limits of secure transmission over fading channels subject to strict deadlines.

Recent works on information theoretic security have been largely motivated by wire-tap channel model [1]. In his seminal work, proved the achievability of non-zero secrecy capacity, assuming that the

wiretapper channel is a degraded version of the main one, by exploiting the noise to create an advantage for the legitimate receiver. The effect of fading on the secrecy capacity was further studied in [2] in the ergodic setting. The main insight offered by this work is that one can opportunistically exploit the fading to achieve a non-zero secrecy capacity even if the eavesdropper channel is better than the legitimate receiver channel, on the average.

Delay limited transmission over fading channels has been well studied in different network settings and using various traffic models. For instance, in [3], the delay constrained limit thought was presented and the ideal power control strategies were portrayed in a few intriguing situations. In [4], the strict delay impediment of [3] was casual by taking into consideration buffering the parcels at the transmitter. In this setup, the asymptotic conduct of the power-

delay exchange off bend was described yielding profitable bits of knowledge on the structure of the ideal asset allotment methodologies [4]. All the more as of late, the booking issue of information transmission over a limited delay skyline accepting impeccable CSI was considered in [5]. Our work can be viewed as a generalization of [3] where a secrecy constraint is imposed on the problem. The extension to the bursty traffic scenario is currently under investigation.

The delay limited transmission of secure data over fading channels was considered previously in [8]. In this work, the authors attempted to send the secure information using binning techniques inspired by the wiretap channel results. The drawback of this approach is that it fails to secure the information in the particular instants where the eavesdropper channel gain is larger than that of the main channel resulting in the so-called secrecy outage phenomenon (as defined in [8]). Unfortunately, in the delay limited setting, the secrecy outage can not made to vanish by increasing the block length leading to the conclusion that the delay limited rate achieved by this approach is equal to zero for most channel distributions of interest [8]. This obstacle is overcome by our two-stage approach. Here, the delay sensitive data of the current block is secured via Vernam's one time pad approach [6], which was proved to achieve perfect secrecy by Shannon [7], where the legitimate nodes agree on the private key during the previous blocks. Since the key packets are not delay sensitive, the two nodes can share the key by distributing its bits over many fading realizations to capitalize on the ergodic behavior of the channel. Through the suitable rate designation, the key bits can be superimposed on the delay delicate information bundles with the goal that they can be utilized for securing future parcels. This is alluded as key reestablishment process in the continuation. This procedure requires an instatement stage to share the key required for securing the primary information bundles. However, the loss in the secrecy entailed by

the initialization overhead vanishes in the asymptotic limit of a large number of data packets. Our analytical results establish the asymptotic optimality, with high SNR, of this novel approach in the scenario where both the main and eavesdropper channel gains are known a-priori at the transmitter (for a wide class of channel distributions). When only the main channel CSI is available, this approach is shown to achieve a non-zero constant secrecy rate for a wide class of quasi-static channels (i.e., the class of invertible channels [3]).

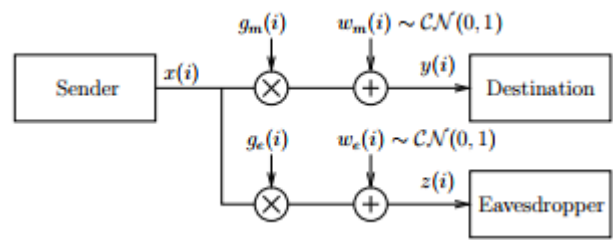


Figure 1. System Model

The rest of the paper is organized as follows. Section II details the system model and the notations used throughout the rest of the paper. In Section III, our main results for both the full and main CSI cases are obtained. Finally, Section IV concludes the paper.

II. SYSTEM MODEL

The system model is as shown in Figure 1. A source node (Alice) communicates with a destination node (Bob) over a fading channel in the presence of an eavesdropper (Eve). I adopt a block fading model, in which the channel is assumed to be constant during a coherence interval and changes randomly from an interval to another according to a bounded continuous distribution. Also the coherent intervals are assumed to be large enough to allow for the use of random coding techniques.

During any coherence symbol interval i , the signals received at the destination and the eavesdropper are given by

$$y(i) = g_m(i)x(i) + w_m(i), \quad (1)$$

$$z(i) = g_e(i)x(i) + w_e(i), \quad (2)$$

where $x(i)$ is the transmitted image, $g_m(i)$ and $g_e(i)$ are the fundamental channel and the spy channel picks up separately, $w_m(i)$ and $w_e(i)$ are the i.i.d.

added substance white complex gaussian commotion with unit fluctuation at the authentic collector and the spy, separately. I denote the power gains of the fading channels for the main and eavesdropper channels by $h_m(i) = |g_m(i)|^2$ and $h_e(i) = |g_e(i)|^2$, respectively. I impose the long term average power constraint P^- , i.e.,

$$\mathbb{E}[P(\mathbf{h})] \leq \bar{P}, \quad (3)$$

where $P(\mathbf{h})$ is the power allocated for the channel state $\mathbf{h} = (h_m, h_e)$ and the expectation is over the channel gains.

The source wishes to send a message $W \in \mathcal{W} = \{1, 2, \dots, M\}$ to the destination. In the following, our delay constraint is imposed by breaking our message into packets of equal sizes, where each one is encoded independently, transmitted in only one coherence block, and decoded by the main receiver at the end of this block. Accordingly, the total number of channel uses is partitioned into b super-blocks. Each super-block is divided into a blocks of n_1 symbols, where $n = b a n_1$ and n_1 denotes the length of coherence intervals. I will further represent a fading block with tuple (m, l) such that $m \in \{1, 2, \dots, b\}$ and $l \in \{1, 2, \dots, a\}$. We consider the problem of constructing (M_1, n_1) codes ($M = b a M_1$) to transmit the message of the block (m, l) , $W(m, l) \in \mathcal{W}_1 = \{1, 2, \dots, M_1\}$ to the receiver. Here, an (M_1, n_1) code consists of the following elements: 1) a stochastic encoder $f_{n_1}(\cdot)$ at the source that maps the message $w(m, l)$ to a codeword $x_{n_1}(m, l) \in \mathcal{X}_{n_1}$, and 2) a decoding function $\varphi: \mathcal{Y}_{n^*} \rightarrow \mathcal{W}_1$ at the legitimate receiver, where $n^* = (m-1)an_1 + n_1$ denotes the total number received signal dimension at the receiver at the end of the block (m, l) . The average error probability of an (M_1, n_1) code is defined as

$$P_e^{n_1} = \frac{1}{M_1} \sum_{w \in \mathcal{W}_1} \Pr(\varphi(y^{n^*}) \neq w | w \text{ was sent}),$$

where y_{n^*} represents the total received signals at the legitimate receiver at the end of the block (m, l) . The equivocation rate R_e at the eavesdropper is

defined as the entropy rate of the transmitted message conditioned on the available CSI and the channel outputs at the eavesdropper, i.e.,

$$R_e \triangleq \frac{1}{n} H(W | Z^n, h_m^n, h_e^n), \quad (4)$$

where $h_m^n = \{h_m(1), \dots, h_m(n)\}$ and $h_e^n = \{h_e(1), \dots, h_e(n)\}$ denote the channel power gains of the legitimate receiver and the eavesdropper in n symbol intervals, respectively. I consider only the perfect secrecy (in the sense of [1]) which requires the equivocation rate R_e to be ϵ close to the message rate. The delay limited perfect secrecy rate $R_{s,d}$ is said to be achievable if for any $\epsilon > 0$, there exists a sequence of codes $(2^{n_1 R_{s,d}}, n_1)$ such that for any $n_1 \geq n_1(\epsilon)$, I have for any fading block (m, l) .

$$\begin{aligned} P_e^{n_1} &\leq \epsilon \\ R_e &\geq R_{s,d} - \epsilon \end{aligned}$$

Finally, we give some notational remarks. I denote the delay limited secrecy rate and capacity as $R(F)_{s,d}$ and $C(F)_{s,d}$ for the full CSI case (both g_m and g_e are known a-priori at the transmitter). I respectively use the notation $R(M)_{s,d}$ and $C(M)_{s,d}$ for the main CSI case (only g_m is known a-priori at the transmitter). I denote $[x]^+ = \max\{x, 0\}$. And, we remark that the expectations are with respect to channel gains throughout the sequel.

III. MAIN RESULTS

A. Full CSI Scenario

First, I give a simple upper bound on the delay limited secrecy capacity that will be used later to establish the optimality of the proposed approach in the high SNR regime.

Theorem 1: The delay-limited secrecy capacity when both g_m and g_e are available at the transmitter, $C(F)_{s,d}$, is upper bounded by

$$C_{s,d}^{(F)} \leq \max_{\substack{P(\mathbf{h}) \\ \text{s.t. } \mathbb{E}[P(\mathbf{h})] \leq P}} \min \{R_s^{(F)}, R_d^{(F)}\}, \quad (5)$$

where $R_s^{(F)}$ and $R_d^{(F)}$ are given as follows.

$$\begin{aligned} R_s^{(F)} &= \mathbb{E} [\log(1 + P(\mathbf{h})h_m) - \log(1 + P(\mathbf{h})h_e)]^+ \\ R_d^{(F)} &= \min_{\mathbf{h}} \log(1 + P(\mathbf{h})h_m) \end{aligned}$$

Proof: For a given power allocation scheme $P(\mathbf{h})$, we have

$$R_{s,d}^{(F)} \leq R_s^{(F)}, \quad (6)$$

for any achievable delay limited secrecy rate $R(F)_{s,d}$, since imposing delay constraint can only degrade the performance. I also have, for a given $P(\mathbf{h})$,

$$R_{s,d}^{(F)} \leq R_d^{(F)}, \quad (7)$$

since imposing secrecy constraint can not increase the achievable rate. Then, combining (6) and (7), and maximizing over $P(\mathbf{h})$, we obtain

$$R_{s,d}^{(F)} \leq \max_{P(\mathbf{h})} \min \{R_d^{(F)}, R_s^{(F)}\}, \quad (8)$$

for any achievable delay-limited secrecy rate $R(F)_{s,d}$, which proves our result.

The accompanying outcome builds up a lower bound on the delay constrained mystery limit utilizing our novel two-organize approach. The key thought is to share a private key amongst Alice and Bob, without being compelled by the delay confinement. Then, this key is used to secure the delay sensitive data to overcome the secrecy outage phenomenon. In the steady state, the key renewal process takes place by superimposing the key on the delay sensitive traffic. More precisely, as outlined in the proof, the delay sensitive traffic (secured by the previous key) serves as a randomization signal in the binning scheme used to secure the current key. At long last, since he is known from the earlier at the transmitter, one can additionally expand the delay restricted mystery rate by committing a part of the protected rate to the delay touchy activity (as controlled by the capacity $q(\mathbf{h})$ in the accompanying hypothesis).

Hypothesis 2: The delay-restricted mystery limit in the full CSI situation is bring down limited as takes after.

$$C_{s,d}^{(F)} \geq R_{s,d}^{(F)} = \max_{\substack{P(\mathbf{h}), q(\mathbf{h}) \\ \text{s.t. } \mathbb{E}[P(\mathbf{h})] \leq P}} \left[\min_{\mathbf{h}} \{R_s''(\mathbf{h}) + R_o(\mathbf{h})\} \right], \quad (9)$$

where

$$\begin{aligned} R_s''(\mathbf{h}) &= R_s(\mathbf{h}) - R_s'(\mathbf{h}), \\ R_s(\mathbf{h}) &= [\log(1 + P(\mathbf{h})h_m) - \log(1 + P(\mathbf{h})h_e)]^+, \\ R_s'(\mathbf{h}) &= [\log(1 + P(\mathbf{h})h_m) - \log(1 + P(\mathbf{h})q(\mathbf{h}))]^+, \end{aligned}$$

such that $q(\mathbf{h})$ is an arbitrary chosen function satisfying $q(\mathbf{h}) \geq h_e \forall h_e$, and R_o is chosen to satisfy the followings.

$$\begin{aligned} \mathbb{E}[R_o(\mathbf{h})] &\leq \mathbb{E}[R_s'(\mathbf{h})] \\ R_o(\mathbf{h}) &\leq \min \{\log(1 + P(\mathbf{h})h_m), \log(1 + P(\mathbf{h})h_e)\} \end{aligned} \quad (10)$$

Sketch of the Proof: In our scheme, I require Alice to transmit a delay constrained data message and a key to Bob. The key is used to encrypt data and thus should be secured from Eve. A given message $w \in \{1, 2, \dots, 2^{n(R(F)_{s,d})}\}$ is transmitted by sending n data packets of equal length, each represented by $D(m, l)$, where each packet is encoded independently and sent with rate $R(F)_{s,d}$ during the corresponding block of the channel. I further divide a packet to be transmitted at block (m, l) into two parts $D1(m, l)$ and $D2(m, l)$. The first part of data packet is transmitted along with the generated key using the one-time pad scheme, whereas the second part is transmitted as a secret message. I use a separation strategy similar to [9] by sending public and private messages simultaneously. But, in contrast to [9], I here have the fading channel as the resource from Alice to Bob and Eve and I exploit it to secure the key, and hence, the message. I now describe the initial key generation and key renewal. For the very first a blocks (the super-block $m = 1$), I transmit the key, $K(1)$, from Alice to Bob securely. Utilizing the ergodicity of the channel, I can transmit a key of length $n\mathbb{E}[R_s'(\mathbf{h})]$ bits [2]. Then, for any super-block m , I will use the key $K(m-1)$ for the one time pad, and also generate a new key $K(m)$ for the use in the next super-block. For any given block (m, l) , we use the $n(1-R_o(\mathbf{h}))$ remaining bits of the key $K(m-1)$ and denote the corresponding bits as $\tilde{K}(m, l)$. These bits are used in a one-time pad scheme to construct $D_o(m, l) = D1(m, l) \oplus \tilde{K}(m, l)$. The encrypted bits are then mapped to a message $w1(m, l) \in \{1, 2, \dots, 2^{n(R(F)_{s,d})}\}$.

$n_1 R_o(\mathbf{h})$. The message w_1 along with a possible additional randomization is transmitted along with the secret data. Here, the secret data I sent within a block is two-fold: $w_2(m, l) \in \{1, 2, \dots, 2(n_1 R'' s(\mathbf{h}))\}$ which carries the corresponding data $D_2(m, l)$ and the key message $w_k(m, l) \in \{1, 2, \dots, 2(n_1 R' s(\mathbf{h}))\}$. These latter messages will allow us to generate the key $K(m)$ of the super block m .

Since $b \rightarrow \infty$, $a \rightarrow \infty$, $n_1 \rightarrow \infty$, it can be easily shown that the rates $R_o(\mathbf{h})$, $R' s(\mathbf{h})$, and $R'' s(\mathbf{h})$ are achievable within a given block. Furthermore, the average key rate, $E[R' s(\mathbf{h})]$, is achievable within any super-block (see, e.g., [2]).

I finally argue that the equivocation rate at the eavesdropper can be made arbitrarily close to the message rate with the proposed scheme. Here, I consider equivocation computation per block, which will imply the equivocation computation for the overall message. For a given block (m, l) , the security of $w_1(m, l)$ follows from the one-time pad encryption (as the key is secured from the eavesdropper [7]) and the security of $w_2(m, l)$ follows from the wire-tap channel result along with the secure rate choice $R' s(\mathbf{h})$ and $R'' s(\mathbf{h})$ [1]. I note that during the first super-block $w_1(1, l)$ is not encrypted. However, this will not affect the overall secrecy of the data as $b \rightarrow \infty$. Hence, the equivocation rate can be made close to the message rate as $b \rightarrow \infty$, $a \rightarrow \infty$, and $n_1 \rightarrow \infty$.

The achievable rate is then minimized over \mathbf{h} to satisfy the delay limitation and then maximized over all power control policies and functions $q(\mathbf{h})$ (used to allocate rate for w_2). This proves the desired result. The final step in this section is to prove the asymptotic optimality of the proposed security scheme in the high SNR regime. The following result establishes this objective by showing that the upper and lower bounds of Theorems 1 and 2 match in this asymptotic scenario.

Lemma 3: In an asymptotic regime of high SNR, i.e., $P^- \rightarrow \infty$, the delay limited secrecy capacity is given by

$$\lim_{P^- \rightarrow \infty} C_{s,d}^{(F)} = E_{h_m > h_e} \left[\log \left(\frac{h_m}{h_e} \right) \right], \quad (11)$$

assuming that $E h \frac{1}{\min(h_e, h_m)}$ is finite. Moreover, the capacity is achieved by the proposed one-time pad encryption scheme coupled with the key renewal process.

Proof: I only need to consider the lower bound since the right hand side of (11) is the ergodic secrecy capacity in the high SNR regime, which is by definition an upper bound on the delay limited secrecy capacity. To this end, we set $q(\mathbf{h}) = h$ resulting in $R'' s(\mathbf{h}) = 0$. Furthermore, we let $P(\mathbf{h}) = c \min(h_e, h_m)$, where c is a constant, which is chosen according to the average power constraint. The achievable rate expression in the high SNR regime is then given by

$$\lim_{P^- \rightarrow \infty} R_{s,d}^{(F)} = \lim_{P^- \rightarrow \infty} \min_{\mathbf{h}} R_o(\mathbf{h}), \quad (12)$$

where $R_o(\mathbf{h})$ is chosen to satisfy

$$\begin{aligned} E[R_o(\mathbf{h})] &\leq E[\log(1 + P(\mathbf{h})h_m) - \log(1 + P(\mathbf{h})h_e)]^+ \\ R_o(\mathbf{h}) &\leq \log(1 + c) \end{aligned} \quad (13)$$

As $P^- \rightarrow \infty$, it is easy to see that $c \rightarrow \infty$ since $E h \frac{1}{\min(h_e, h_m)}$ is finite, implying that the second constraint in (13) is loose. Ao, it is easy to see that the first constraint converges to the right hand side of the lemma. Then, by choosing $R_o(\mathbf{h}) = E_{h_m > h_e} h \log \frac{h_m}{h_e}$, both constraints of (13) are satisfied and our result is proved.

The above claim is validated numerically in Fig. 2, where Chi-square distribution of degree $n = 4$ is used for the statistics of channel gains of the legitimate receiver and the eavesdropper (the gains are assumed to be independent). In our simulation, I set $q(\mathbf{h}) = h$ (hence $R'' s = 0$) and use channel inversion power control policy for the achievable rate. Remarkably, even with the suboptimal choice of $q(\mathbf{h})$ and $P(\mathbf{h})$,

lower and upper bounds coincides at the high SNR regime.

IV. CONCLUSION

The delay-limited secrecy capacity of the slow-fading channel under different assumptions on the CSI at the transmitter. Our achievability arguments are based on

A novel two-arrange plot that takes into account conquering the mystery blackout marvel for a wide class of channels. The plan depends on sharing a delay tolerant private key, utilizing arbitrary binning, and after that utilizing the way to scramble the delay touchy parcels in a one time cushion organize. For the full CSI case, our scheme is further shown to be asymptotically optimal, i.e., high SNR regime, for many relevant channel distributions. When only the main channel CSI is available, the two-stage scheme achieves a non-zero secure rate, under a strict delay constraint, for invertible channels. Finally, one can easily identify avenues for future works; three of them are immediate, namely 1) obtaining sharp capacity results for finite values of SNR, 2) characterizing the optimal power control policies, and 3) extending the framework to bursty traffic by allowing for buffer delays.

V. REFERENCES

- [1]. A. D. Wyner, "The Wire-Tap Channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
- [2]. P. K. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," IEEE Trans. on Inf. Theory, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.
- [3]. S. V. Hanly and D. N. C. Tse "Multiaccess Fading Channels-Part II: Delay-Limited Capacities," IEEE Trans. on Inf. Theory, vol. 44, no. 7, pp. 2816-2831, Nov. 1998.
- [4]. R. A. Berry and R. G. Gallager, "Communication Over Fading Channels with Delay Constraints," IEEE Trans. on Inf. Theory, vol. 48, no. 5, pp. 1135-1149, May 2002.

- [5]. J. Lee and N. Jindal, "Energy-efficient Scheduling of Delay Constrained Traffic over Fading Channels," IEEE Trans. on Wireless Communications, to appear.
- [6]. G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," J. Amer. Inst. Elect. Eng., vol. 55, pp. 109-115, 1926.
- [7]. C. E. Shannon, "Communication Theory of Secrecy Systems," The Bell System Technical Journal, vol. 28, pp. 656-715, Oct. 1949.
- [8]. M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," IEEE Trans. on Inf. Theory, volume 54, no. 6, pp. 2515-2534, June 2008.
- [9]. V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via Sources and Channels-A Secret Key - Secret Message Rate Tradeoff Region," in Proc. of IEEE International Symposium on Information Theory (ISIT'08), Toronto, ON, Canada, July 2008.

ABOUT AUTHORS:



B.kavitha is currently pursuing her MCA department, St. Ann's college of Engineering & Technology, Chirala. AP. She received her B.Sc computer science degree from AMG Degree for

women in Chilakaluri pet.



Dr.K.S. Yuvaraj Ph.D in computer science, specialization advanced networking and working as an Associate Professor in Department of Computer Science Engineering, St. Ann's college of Engineering and

Technology, Chirala, AP.