Secure Joint Source-Channel Coding for Quasi-Static Fading Channels

Tony Q.S. Quek  
Institute for Infocomm Research  
1 Fusionopolis Way, #21-01 Connexis  
Singapore 138632  
e-mail: qsquek@i2r.a-star.edu.sg

Kiran Thimme Gowda  
Mobile Communications Department  
Eurécom Institute  
06904 Sophia-Antipolis, France  
e-mail: kiran.gowda@eurecom.fr

Hyundong Shin  
School of Electronics and Information  
Kyung Hee University  
Gyeonggi-do, Korea  
e-mail: hshin@khu.ac.kr

Abstract—Joint source-channel coding has been shown to yield optimal end-to-end performance in terms of overall expected distortion for quasi-static fading channels. Due to the inherent broadcast nature of the wireless medium, wireless communications are susceptible to eavesdropping. Thus, it is unclear how imposing additional secrecy constraint on the system will affect the end-to-end performance of the joint source-channel coding. In this paper, we consider the information theoretic secure source transmission in a classical three node wiretap channel, consisting of a source node, a destination node, and a wiretapper node. In the high signal-to-noise ratio regime, we quantify the cost of providing secure transmissions through secrecy outage probability and secrecy distortion exponent. Our results show that with the additional secrecy constraint, there exists a lower bound on the bandwidth expansion factor, below which perfect secrecy is impossible. Moreover, this lower bound on bandwidth expansion factor depends on the type of layered source transmission strategy used. In summary, this work indicates that source-channel coding strategies as well as the level of secrecy need to be carefully designed in order to maximize the secrecy distortion exponent.

I. INTRODUCTION

Unlike wire-line networks, the broadcast nature of wireless medium presents exciting challenges to the design of efficient wireless networks. Of particular interest is the vulnerability of wireless networks to eavesdropping and security attacks. Therefore, ensuring network robustness against various types of security threats is one of the important design objective of wireless networks. Traditionally, this issue has been addressed by employing cryptographic protocols that are believed to be computationally hard for the adversary to decipher. However, as wiretappers and attackers are becoming smarter, there is a recent interest to exploit the physical-layer properties to enhance security, where the secrecy may be embodied within the information itself and also adapted to the channel conditions.

This notion of physical-layer security dates back to Shannon and Wyner, who laid the early foundations for information theoretic security [1], [2]. While Shannon’s model assumed that both the destination channel and the wiretapper channel are noiseless, Wyner considered a more realistic model and showed that positive secrecy capacity can be achieved when the wiretapper channel is physically degraded with respect to the destination channel. Recently, this problem has gained considerable attention due to the proliferation of ad-hoc and sensor networks, where physical layer security may be effective in providing additional security [3]–[9].

In this paper, we consider the transmission of a continuous amplitude source over quasi-static Rayleigh fading channels, where the channel state information (CSI) is available only at the receiver but not at the transmitter. In this case, we can no longer apply Shannon’s source-channel separation theorem and we need to employ joint source-channel coding to minimize the overall expected distortion [10]–[12]. Furthermore, we impose an additional secrecy constraint on the system and consider the information theoretic secure source transmission in a classical three node wiretap channel. For source transmissions, we consider only the case when the signal is encoded into two successive refinement layers, i.e. base and enhancement layers.1 These different layers are transmitted at different transmission rates and different channel uses if progressive transmission is used or transmitted with different power if superposition coding is used as the layered source transmission strategy. In the high signal-to-noise ratio (SNR) regime, we quantify the cost of providing secure transmissions through secrecy outage probability and secrecy distortion exponent. Our results show that with the additional secrecy constraint, there exists a lower bound on the bandwidth expansion factor, below which perfect secrecy is impossible. Moreover, this lower bound on bandwidth expansion factor depends on the type of layered source transmission strategy used. In summary, this work indicates that source-channel coding strategies as well as the level of secrecy need to be carefully designed in order to maximize the secrecy distortion exponent.

II. SYSTEM MODEL

We assume the transmission of a successively refinable, memoryless, zero mean, unit variance complex Gaussian source over a fading channel to the destination. At the destination, we can define the single-letter squared-error distortion between the source vector \(s \in \mathbb{C}^K\) and

\[d(s, s') = |s - s'|^2\]
its reconstruction vector  \( \hat{s} = [\hat{s}_1, \hat{s}_2, \ldots, \hat{s}_K] \in \mathbb{C}^K \) as
\[
D(s, \hat{s}) = \frac{1}{K} \sum_{k=1}^{K} d(s_k, \hat{s}_k) \tag{1}
\]
where \( d(s_k, \hat{s}_k) = |s_k - \hat{s}_k|^2 \) and \( K \) is the source block length. The corresponding distortion-rate function is given by \( D(R) = 2^{-R} \), where \( R \) is the source coding rate in bits/symbol [13]. Furthermore, we consider a block fading channel model parameterized by a finite and fixed coherence time [14]. The channel is partitioned into multiple flat fading blocks, where the channel fading coefficient \( h \) within each block of length \( L \) is constant. Typically, we can model each random channel coefficient as a circularly symmetric complex Gaussian random variable (r.v.), i.e., \( h \sim \mathcal{CN}(0, \sigma_h^2) \), where \( \mathcal{CN}(\mu, \sigma^2) \) denotes a complex circularly symmetric Gaussian distribution with mean \( \mu \) and variance \( \sigma^2 \). We assume that a source realization of \( K \) symbols are encoded and transmitted over each fading block. Therefore, we can define a bandwidth expansion factor of \( b = L/K \), leading to a channel code of rate \( R/b \) bits/channel use. In the quasi-static fading scenario, once a channel is in deep fade, coding no longer helps to increase the reliability of the transmission. In this case, the natural performance measure becomes the outage probability. Here, we assume that the perfect CSI is not available at the source, but only at the destination.

Considering a three-node wireless network with a single transmitter (Alice), an intended receiver (Bob), and an eavesdropper (Eve). In this setup, we are interested to protect the message sent from Alice to Bob against Eve such that the dropper (Eve). In this setup, we are interested to protect the transmitter (Alice), an intended receiver (Bob), and an eavesdropper (Eve) within each fading block and  \( z \) is the source block length where \( z \) is the source block length. Therefore, we can define a bandwidth expansion factor of \( b = L/K \), leading to a channel code of rate \( R/b \) bits/channel use. In the quasi-static fading scenario, once a channel is in deep fade, coding no longer helps to increase the reliability of the transmission. In this case, the natural performance measure becomes the outage probability. Here, we assume that the perfect CSI is not available at the source, but only at the destination.

Within each fading block, the received signal for the  \( t \)th channel symbol at Bob is given by
\[
y_{b,t} = h x_t + z_{b,t} \tag{2}
\]
where \( l = 1, 2, \ldots, L \), \( x_t \in \mathbb{C} \) is the transmitted transmitted, and \( z_{b,t} \sim \mathcal{CN}(0, \sigma_B^2) \) denotes the circularly symmetric complex Gaussian noise at Bob. In addition, we let \( x_t \sim \mathcal{CN}(0, P) \) such that \( \sum_{t=1}^{L} \mathbb{E}\{|x_t|^2\} \leq LP \). Similarly, Eve receives an independent copy of the message from Alice and its received signal is given by
\[
y_{e,t} = g x_t + z_{e,t} \tag{3}
\]
where \( g \) denotes the random channel coefficient from Alice to Eve within each fading block and \( z_{e,t} \sim \mathcal{CN}(0, \sigma_E^2) \) denotes the circularly symmetric complex Gaussian noise at Eve. For notational convenience, we define \( \text{SNR} = P/\sigma_B^2 \).

Following [4], we consider the secrecy capacity \( C_s \) of this three-node network and assume that Bob and Eve have perfect knowledge of their respective receive channel fading coefficients. The measure of secrecy at the wiretapper is the equivocation rate \( \frac{1}{L} H(W|y_E, g) \), where \( W \) is the transmitted message and \( y_E \) is the the received signal sequence at the wiretapper [2]. A rate-equivocation pair \( (R, \delta) \) is said to be achievable if \( \frac{1}{L} H(W|y_E) = \delta \) and the error probability at the destination node simultaneously approaches zero. The system performance measure for a wiretap channel is the rate-equivocation region, which indicates a tradeoff between transmission rates and the level of achievable security. An operating point in this region is said to be perfectly secure if the achieved equivocation rate is arbitrarily close to the rate of information transmission. The largest perfectly secure rate is called the secrecy capacity. Therefore, conditioned on \( h \) and \( g \), the perfect secrecy capacity is given by
\[
C_s = \begin{cases} 
\log(1 + |h|^2 \text{SNR}) - \log \left( 1 + \frac{\sigma_B^2 |g|^2}{\text{SNR}} \right), & \text{if } |h|^2 \geq \frac{\sigma_B^2 |g|^2}{\text{SNR}} \\
0, & \text{if } |h|^2 < \frac{\sigma_B^2 |g|^2}{\text{SNR}}.
\end{cases}
\tag{4}
\]

For such a model, the system is said to fail if the wiretapper equivocation rate is non-zero. With a target perfectly secrecy rate \( R_s \), we call this failure event as the secrecy outage event and investigate the high SNR behavior of this secrecy outage probability. When the perfectly secrecy rate \( R_s \) scales with the SNR, we say a secure diversity-multiplexing gain pair \( (d(r_s), r_s) \) is achievable if
\[
R_s = r_s \log \text{SNR} \quad \& \quad P_{\text{out}}(\text{SNR}) = \text{SNR}^{-d(r_s)}
\]
where \( P_{\text{out}}(\text{SNR}) \) denotes the secrecy outage probability at Bob. The notation \( \cong \) denotes exponential equality and we mean that
\[
f(\text{SNR}) \cong \text{SNR}^x \iff \lim_{\text{SNR} \to \infty} \frac{\log f(\text{SNR})}{\log \text{SNR}} = x.
\]

Under this secrecy constraint, we want to characterize the end-to-end expected distortion (ED), \( \mathbb{E}\{D(s, \hat{s})\} \), where the expectation is over the source samples, the channel fading, and the noise distributions. Moreover, our main focus is on the high SNR behavior of the expected distortion, which can be captured in the secrecy distortion exponent \( \Delta \) defined as follows:
\[
\text{ED} \cong \text{SNR}^{-\Delta}.
\]

In this way, we can characterize the tradeoff between secrecy and distortion through the bandwidth ratio and distortion exponent in the high SNR regime.

### III. Secrecy Single-Rate Source and Channel Coding

First, we begin with the distortion exponent analysis for single-rate source and channel coding in a three-node wiretap fading channel. In this case, we assume a wiretap channel code of rate \( R_s \) bits per channel use and the corresponding source coding rate is \( bR_s \) bits per source sample with a bandwidth

\[\text{All the logarithms are to the base } 2 \text{ and the capacity is measured in units of bits per second.}\]

\[\text{Note that exponential inequalities } \leq \text{ and } \geq \text{ are defined similarly.}\]
expansion factor \( b \). For a given \( b \), we denote the secrecy distortion exponent achieved by single-rate source and channel coding for degraded and non-degraded wiretap channels (refer to Figs. 1(a) and 1(b)) as \( \Delta_d \) and \( \Delta_{nd} \), respectively.

**Theorem 1:** For single-rate source and channel coding, the secrecy distortion exponent for a degraded wiretap fading channel is given by

\[
\Delta_d = \frac{b}{1 + b} \quad \text{for} \quad b > \frac{\log SNR}{\log(1 + (\sigma_B^2/\sigma_E^2))} - 1
\]

**Proof:** For a degraded wiretap fading channel, we consider \( g = e^{j\theta} \) such that \( E\{|g|^2\} = 1 \) and \( \theta \) is a random phase uniformly distributed over 0 to \( 2\pi \). Following [11], the expected distortion for single-rate transmission can be written as

\[
ED = (1 - P_{out}(SNR))D(bR_s) + P_{out}(SNR)
\]

where we let \( R_s = r_s \log SNR \) such that \( r_s \in [0,1] \) is the secrecy multiplexing gain and the secrecy outage probability \( P_{out}(SNR) \) is given by

\[
P_{out}(SNR) = \mathbb{P}\left\{ \log \frac{1 + |h|^2SNR}{1 + |h|^2\frac{\sigma_B^2}{\sigma_E^2}SNR} < R_s \right\}
\]

\[
\approx \frac{\sigma_B^2}{SNR \left( 1 - SNR^{r_s} \frac{\sigma_B^2}{\sigma_B^2 + \sigma_E^2} \right)} (SNR^{r_s} - 1)
\]

and \( D(bR_s) \) is the rate-distortion function of the Gaussian source. Here, we assume that the receiver simply outputs the average value of the source distortion of 1 in the case of an outage. For \( P_{out}(SNR) \) in (6) to be positive, we need to have \( 1 - SNR^{r_s} \frac{\sigma_B^2}{\sigma_B^2 + \sigma_E^2} > 0 \), which is equivalent to \( SNR^{-r_s} > \frac{\sigma_B^2}{\sigma_B^2 + \sigma_E^2} \). In this case, we have \( P_{out}(SNR) \approx SNR^{-r_s} \). Therefore, at high SNR, (5) can be approximated as

\[
ED \approx SNR^{-br_s} + P_{out}(SNR)
\]

for \( r_s < \frac{\log(1 + (\sigma_B^2/\sigma_E^2))}{\log SNR} \). Since the highest distortion exponent is achieved when the two exponents in (7) are equal, we have \( r_s^* = \frac{1}{1 + b} \) for \( b > \frac{\log(1 + (\sigma_B^2/\sigma_E^2))}{\log SNR} - 1 \). As a result, the secrecy distortion exponent follows straightforwardly as \( \Delta_d = 1 - r_s^* \).

**Theorem 2:** For single-rate source and channel coding, the secrecy distortion exponent for a non-degraded wiretap fading channel is given by

\[
\Delta_{nd} = \frac{b}{1 + b} \quad \text{for} \quad b > \frac{\log SNR}{\log \lambda_h - \log \lambda_g} - 1
\]

where \(|h|^2 \sim \mathcal{E}(1/\sigma_h^2)\), \(|g|^2 \sim \mathcal{E}(1/\sigma_g^2)\), \( \lambda_h = \frac{\sigma_h^2}{\sigma_E^2} \), and \( \lambda_g = \frac{\sigma_g^2}{\sigma_E^2} \).

**Proof:** For a non-degraded wiretap fading channel, we consider \(|h|^2 \sim \mathcal{E}(1/\sigma_h^2)\), \(|g|^2 \sim \mathcal{E}(1/\sigma_g^2)\). From the proof of Theorem 1, the expected distortion at high SNR can be approximated as

\[
ED \approx SNR^{-br_s} + P_{out}(SNR)
\]

where \( P_{out}(SNR) \) is now given by

\[
P_{out}(SNR) = \mathbb{P}\left\{ \log \frac{1 + |h|^2SNR}{1 + |h|^2\frac{\sigma_B^2}{\sigma_E^2}SNR} < R_s \right\}
\]

\[
= 1 - \frac{\sigma_B^2}{\sigma_B^2 + SNR^{r_s}\frac{\sigma_B^2}{\sigma_E^2}} \exp \left( -\frac{SNR^{r_s} - 1}{SNR\sigma_B^2} \right)
\]

In order for \( P_{out}(SNR) \to 0 \) as \( SNR \to \infty \) in (9), we need to have

\[
1 + SNR^{r_s}\frac{\sigma_B^2}{\lambda_h} \to 1 \quad \text{as} \quad SNR \to \infty
\]

which implies that

\[
\lim_{SNR \to \infty} SNR^{r_s+\varepsilon_h} = 0 \quad \text{for} \quad r_s + \varepsilon_h < 0
\]

where \( \lambda_h = SNR^{\varepsilon_h} \) and \( \lambda_g = SNR^{\varepsilon_g} \) such that \( \varepsilon_h, \varepsilon_g \in \mathbb{R} \). When (11) is satisfied, we have \( P_{out}(SNR) \approx SNR^{-r_s} \). Similar to the proof of Theorem 1 and (11), the highest distortion exponent is given by

\[
r_s^* = \frac{1}{1 + b} \quad \text{for} \quad b > \frac{\log SNR}{\log \lambda_h - \log \lambda_g} - 1
\]

As a result, the secrecy distortion exponent follows straightforwardly as \( \Delta_{nd} = 1 - r_s^* = \frac{b}{1 + b} \).

\[\overset{6}{\text{We have used the notation } X \sim \mathcal{E}(\beta) \text{ to denote that } X \text{ is exponential distributed with a constant hazard rate } \beta > 0.}\]
Remark 1: Our results show that with the additional secrecy constraint, there exists a lower bound on the bandwidth expansion factor, below which perfect secrecy is impossible. However, such a lower bound does not exist for joint source-channel coding without wiretapper.

IV. SECRECY LAYERED SOURCE WITH PROGRESSIVE TRANSMISSION

In layered source with progressive transmission, the source is compressed into two layers, namely base and enhancement layers. The $L$ channel uses are divided into two portions as shown in Fig. 2(a). In the first portion, the base layer is transmitted in the first $\alpha L$ channel uses at secrecy rate $R_s^{(b)}$, where $\alpha \in (0, 1]$. In the second portion, the enhancement layer is transmitted in the rest of channel uses at secrecy rate $R_s^{(e)}$. At Bob, the received signal is obtained by first decoding the base layer following by the enhancement layer from the associated channel uses. Therefore, the overall expected distortion is given by [10]

$$
ED = (1 - P_{\text{out}}^{(e)})D(abR_s^{(b)} + (1 - \alpha)bR_s^{(e)}) + (P_{\text{out}}^{(e)} - P_{\text{out}}^{(b)})D(abR_s^{(b)}) + P_{\text{out}}^{(b)} \tag{13}
$$

where $P_{\text{out}}^{(b)}$ and $P_{\text{out}}^{(e)}$ denote the secrecy outage probabilities associated with the base and enhancement layers, respectively.

**Theorem 3:** For layered source and channel coding with progressive transmission, the secrecy distortion exponent for a degraded wiretapi channel is given by

$$
\Delta_d = 1 - \frac{1}{\left(1 + \frac{b}{\beta}\right)^2} \text{ for } b > 2 \left[ \frac{\log \text{SNR}}{\log (1 + (\sigma^2_B/\sigma^2_H))} - 1 \right].
$$

**Proof:** Similar to the proof of Theorem 1, we let $g = e^{j\theta}$ such that $\mathbb{E}\{|g|^2\} = 1$ and $\theta \in [0, 2\pi]$, and $R_s^{(b)} = r_s^{(b)} \log \text{SNR}$ and $R_s^{(e)} = r_s^{(e)} \log \text{SNR}$, where $r_s^{(b)}, r_s^{(e)} \in [0, 1]$. In addition, the secrecy outage probabilities in (13) can be approximated following the proof in Theorem 1 as follows:

$$
P_{\text{out}}^{(b)} \doteq \text{SNR}^{r_s^{(b)} - 1} \text{ for } r_s^{(b)} < \frac{\log (1 + (\sigma^2_B/\sigma^2_H))}{\log \text{SNR}} \tag{14}
$$

$$
P_{\text{out}}^{(e)} \doteq \text{SNR}^{r_s^{(e)} - 1} \text{ for } r_s^{(e)} < \frac{\log (1 + (\sigma^2_B/\sigma^2_H))}{\log \text{SNR}} \tag{15}
$$

Therefore, at high SNR, (13) can be approximated as

$$
ED \doteq \text{SNR}^{r_s^{(b)} + (1 - \alpha)r_s^{(e)}} + \text{SNR}^{r_s^{(e)} - 1 - \alpha r_s^{(e)}} + \text{SNR}^{r_s^{(b)} - 1} \tag{16}
$$

for $r_s^{(b)} < \frac{\log (1 + (\sigma^2_B/\sigma^2_H))}{\log \text{SNR}}$ and $r_s^{(e)} < \frac{\log (1 + (\sigma^2_B/\sigma^2_H))}{\log \text{SNR}}$.

By equating all the exponents in (16) to be the same, we have

$$
\Delta_d = 1 - \frac{1}{\left(1 + \frac{b}{\beta}\right)^2} \text{ with } \alpha = 1/2. \text{ From (14) and (16), we have } r_s^{(b)} = \frac{1}{1 + b/2\beta} \text{ for } b > \sqrt{\frac{\log \text{SNR}}{\log (1 + (\sigma^2_B/\sigma^2_H))}} - 1.
$$

Furthermore, from (15) and (16), we have $r_s^{(e)} = \frac{1}{1 + b/2\beta}$ for $b > 2 \left[ \frac{\log \text{SNR}}{\log (1 + (\sigma^2_B/\sigma^2_H))} - 1 \right]$. Combining these two bounds on $b$, we have the results in Theorem 3.

**Remark 2:** Comparing to single-rate case, the secrecy layered source with progressive transmission achieves a lower expected distortion at the expense of requiring a larger bandwidth expansion factor. Thus, depending on the operating SNR and system parameters, it may only be feasible to employ secure single-rate source and channel coding. Moreover, note that there is no lower bound on $b$ for progressive transmission without wiretapper.

V. SECRECY LAYERED SOURCE WITH SUPERPOSITION TRANSMISSION

In layered source with superposition transmission, the two layers are transmitted over $L$ channel uses by superimposing a secrecy code at rate $R_s^{(e)}$ for the enhancement layer on top of.
for superposition transmission, the secrecy distortion exponent for the enhancement layer when the base layer is removed from the received signal.

Theorem 5: For layered source and channel coding with superposition transmission, the secrecy distortion exponent for a non-degraded wiretap fading channel is given by

\[ \Delta_{\text{nd}} = 1 - \frac{1}{1 + b + b^2} \text{ for } b > \sqrt{\frac{\log \text{SNR}}{\log \lambda_{\text{b}} - \log \lambda_{\text{g}}} - 1}. \]

**Proof:** For brevity, we omit the proof since it is straightforward from the proof of Theorem 4 and the same argument as in the proof of Theorem 5. \( \square \)

**VI. NUMERICAL RESULTS**

We consider the distance between Alice and Bob is normalized to one and SNR is equivalent to the average received SNR at Bob. In Fig. 3, we show the secrecy exponent for different transmission schemes versus the bandwidth expansion factor \( b \). As expected, this result is similar to the results found in \([10]–[12]\), except each point in the exponent-bandwidth expansion factor curve is achievable if \( b > \frac{1}{1 + b + b^2} \) for \( b > \frac{\log \text{SNR}}{\log \lambda_{\text{b}} - \log \lambda_{\text{g}}} - 1 \). \( \square \)

![Fig. 3. Secrecy distortion exponent.](image-url)
the non-degraded case. From these figures, we see that with additional secrecy constraint there is a certain operating SNR depending on the ratio of $\sigma^2_E$ and $\sigma^2_B$. When $\sigma^2_E/\sigma^2_B$ is small, the main channel is much noisier than the wiretap channel, a higher bandwidth expansion factor is needed to achieve perfect secrecy for a given SNR. However, this requirement on the minimum secrecy bandwidth expansion factor becomes smaller as $\sigma^2_E/\sigma^2_B$ becomes larger, which coincides with our intuition that better secrecy can be achieved when the wiretap channel is degraded with respect to the main channel.

VII. CONCLUSION

In this paper, we considered the information theoretic secure source transmission in a classical three node wiretap channel. In the high signal-to-noise ratio regime, we quantified the cost of providing secure transmissions through secrecy outage probability and secrecy distortion exponent. Our results showed that with the additional secrecy constraint, there exists a lower bound on the bandwidth expansion factor, below which perfect secrecy is impossible. Moreover, this lower bound on bandwidth expansion factor depends on the type of layered source transmission strategy used. In summary, this work indicates that source-channel coding strategies as well as the level of secrecy need to be carefully designed in order to maximize the secrecy distortion exponent.

ACKNOWLEDGMENT

This work was supported in part by the IT R&D program of MKE/IITA [2008-F-005-01, Game Theoretic Approach for Cross-layer Design in Wireless Communications] and the Korea Research Foundation (KRF) grant funded by the Korea government (MEST) (No. 2009-0075941).

REFERENCES