RELIABLE AND SECURE TRANSMISSION FOR FUTURE NETWORKS

Yingbo Hua

University of California at Riverside

yhua@ece.ucr.edu

April 2020 - Slides for ICASSP2020 Online Presentation

Overview

1. Abstract
2. Introduction
3. A Novel Physical Layer Encryption Method (RRCM)
4. Eve's Challenge to Break RRCM
5. Final Remarks

Abstract

- This paper introduces a novel physical layer encryption method called randomized reciprocal channel modulation (RRCM) for reliable and secure transmission (RESET) of information against eavesdropper (Eve) with any number of antennas and any noise level.
- RRCM makes it computationally complex for Eve to estimate the user's channel state information (CSI) that is used to scramble the information symbols transmitted between users.
- Subject to Eve's failure to overcome the physical-layer computational complexity, RRCM can yield a virtually constant (significant) rate in bits/s/Hz of unconditional secrecy - unconditional on Eve's number of antennas, Eve's noise level and the CSI coherence time.

Introduction

- Future wireless networks promise to provide ultra fast communications among billions of people and trillions of things around the world. Yet, questions on security issues are abundant, which hinders the development of ultra fast networks for the benefit of humanity.
- One important security issue is privacy. Future networks will continue to rely on intermediate nodes to store and relay information transmitted from one user (Alice) to another (Bob). Every such transmission leaves the original information somewhere on the trail.
- To ensure end-to-end security, Alice and Bob must share a secret that is needed to encrypt their information.
- Then how can Alice and Bob achieve a shared secret in the first place without inconvenient physical contact? Or how can they achieve this whenever they are within each other's radio range?

Introduction (Cont.1)

- Methods of physical layer security [1] are available to establish or transmit secret information between users, which include such methods as beamforming, artificial noise and cooperative nodes.
- But most of the existing methods fail to yield a positive secrecy when an eavesdropper (Eve) has a large number of antennas or a very low noise level. Also, many methods are unable to handle covert Eve whose channel state information (CSI) is kept unknown to users
- For strong security, we need to develop methods that can yield positive unconditional secrecy (UNS) - unconditional on Eve's channel condition such as its number of antennas and noise level.
- A class of methods that can yield positive UNS is based on user's (reciprocal) CSI which is uncorrelated with Eve's CSI. For these methods, however, the UNS per channel coherence period is also known [2] to be upper bounded by the entropy $H(S)$ of user's CSI.

Introduction (Cont.2)

- In this paper, we are interested in achieving a virtual UNS that is not bounded by the strict UNS $H(S)$.
- A virtual UNS of a scheme is the minimum secrecy of the scheme in the presence of Eve with any number of antennas and any noise level, subject to Eve's failure to overcome the physical layer computational complexity imposed by the scheme.
- This paper introduces the randomized reciprocal channel modulation (RRCM) scheme. The RRCM scheme is a physical layer encryption method but differs from a prior method in [3]. The latter requires Eve's CSI to be unknown to Eve. Such an assumption is problematic for microwave/mmw radios where pilots are required for reliable transmission. (For full-duplex radio, however, anti-eavesdropping channel estimation using pilots is available in [4].)

RRCM for SISO User Channel

- Consider a SISO user channel between two half-duplex users where Alice plans to transmit secret information to Bob where Eve may have any number of antennas, any noise level and be located anywhere (except a fraction of wavelength away from each user).

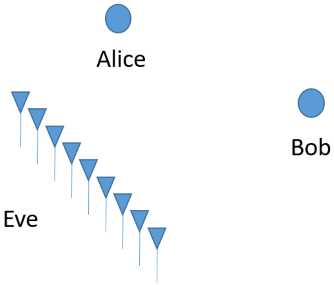

Figure: Achieving a virtually constant (significant) rate of unconditional secrecy against eavesdropper who may have any number of antennas and any noise level.

RRCM for SISO User Channel (Cont.1)

- In coherence period 1, Bob first transmits a pure (publicly known) pilot $p(n)$ so that Alice can estimate the reciprocal channel gain h_1 between Alice and Bob. (At the same time, we know that Eve can obtain its receive channel vector $\mathbf{g}_{B,1}$ with respect to Bob.)
- After that, Alice transmits a sequence of randomized pilots as follows:

$$m_{1,1}p(n), m_{1,2}p(n), \cdots, m_{1,S}p(n) \tag{1}$$

  where $m_{1,s}$ for all s are complex factors randomly generated by Alice.
- Then, Bob can perform channel estimation to obtain $h_1 m_{1,s}$ for all s, and Eve can obtain $\mathbf{g}_{A,1} m_{1,s}$ for all s where $\mathbf{g}_{A,1}$ is Eve's receive channel vector with respect to Alice.
- The above process is repeated in channel coherence periods 2, 3 and 4.

RRCM for SISO User Channel (Cont.2)

- At a time within period 4, both Alice and Bob have obtained $h_1 m_{1,s}, h_2 m_{2,s}, h_3 m_{3,s}, h_4 m_{4,s}$ for $s = 1, \cdots, S$, and they both know all components in the following SVD:

$$\left[\begin{array}{cc} h_1 m_{1,s} & h_2 m_{2,s} \\ h_3 m_{3,s} & h_4 m_{4,s} \end{array} \right] = \sigma_{1,s} \mathbf{u}_{1,s} \mathbf{v}_{1,s} + \sigma_{2,s} \mathbf{u}_{2,s} \mathbf{v}_{2,s}. \tag{2}$$

- Alice chooses and Bob knows the randomized modulation factors as follow:

$$\bar{m}_s = \sigma_{1,s} e^{j\mu_{1,s}} \tag{3}$$

where $\mu_{1,s}$ can be chosen to be the phase of the first element of $\mathbf{u}_{1,s}$.

RRCM for SISO User Channel (Cont.3)

- But Eve at best knows $\mathbf{g}_{A,1}m_{1,s}, \mathbf{g}_{A,2}m_{2,s}, \mathbf{g}_{A,3}m_{3,s}, \mathbf{g}_{A,4}m_{4,s}$ for all s, from which (via a common subspace of $\mathbf{g}_{A,i}m_{i,s}$ for all s and each i) Eve can compute $\hat{m}_{i,s} = g_i m_{i,s}$ for all i and all s where g_i is an ambiguity factor unknown to Eve.
- The left-hand-side matrix of the SVD equation (2) is equivalent to

$$\begin{bmatrix} h_1 m_{1,s} & h_2 m_{2,s} \\ h_3 m_{3,s} & h_4 m_{4,s} \end{bmatrix} = \begin{bmatrix} \frac{h_1}{g_1}\hat{m}_{1,s} & \frac{h_2}{g_2}\hat{m}_{2,s} \\ \frac{h_3}{g_3}\hat{m}_{3,s} & \frac{h_4}{g_4}\hat{m}_{4,s} \end{bmatrix} \quad (4)$$

  where $\frac{h_i}{g_i}$ for each i is a lumped ambiguity factor for Eve.
- Since $\frac{h_i}{g_i}$ is unknown to Eve, Eve is unable to determine any $\bar{m}_s$ from its knowledge of $\hat{m}_{i,s}$.

RRCM for SISO User Channel (Cont.4)

- With $\bar{m}_s$ for all s in period 4, Alice transmits the following within period 4:
$$p(n), \bar{m}_1 c_1, \bar{m}_2 c_2, \cdots, \bar{m}_S c_S \tag{5}$$
where c_s for all s are information symbols.
- Corresponding to $p(n)$ in the above string of symbols, Bob can estimate h_4.
- Corresponding to $\bar{m}_s c_s$ in the above, Bob receives
$$y_{B,s} = h_4 \bar{m}_s c_s + w_{B,s} \tag{6}$$
where $w_{B,s}$ is the noise (including all perturbations due to channel estimation errors). Since Bob knows $h_4 \bar{m}_s$, Bob can estimate and detect the digital information in c_s for all s.
- The above signal model is equivalent to a fast-fading channel with all fading parameters known in advance to the transmitter (Alice) and the receiver (Bob).

RRCM for SISO User Channel (Cont.5)

- In parallel to what Bob has done, Eve can estimate $\mathbf{g}_{A,4}$ and also receives
$$\mathbf{y}_{E,s} = \mathbf{g}_{A,4} \bar{m}_s c_s + \mathbf{w}_{E,s} \tag{7}$$
for all s, where $\bar{m}_s$ is unknown to Eve. Since $\bar{m}_s$ for all s can be chosen by Alice in a random fashion to mask the information in c_s for all s, Eve is blind to the information in c_s.
- Subject to Eve's failure to compute $\bar{m}_s$, all information transmitted from Alice to Bob is in a virtual unconditional secrecy from Eve (unconditional on Eve's number of antennas and noise level).
- The above process in period 4 can be repeated in period 5 and beyond.
- For SISO user channel, there is an initial overhead of three coherence periods. This overhead becomes negligible after a large number of periods.

Eve's Challenge to Break RRCM

- In the case of SISO user channel, Eve has to randomly guess c_s (or equivalently $\bar{m}_s$) for $s = 1, \cdots, S_0$ with $S_0 \geq 4$. And then for each guess of these symbols, Eve has to compute the inverse of a set of nonlinear equations governed by the SVD to determine $\frac{h_1}{g_1}, \frac{h_2}{g_2}, \frac{h_3}{g_3}, \frac{h_4}{g_4}$.
- The strict UNS per coherence period is strictly positive, and "typically" equals the entropy of one information symbol c_s.
- The computational complexity of the inverse is high. If Newton's method is applied, there are many incorrect local solutions and each iteration has a complexity order equal to $\mathcal{O}(N_{unk}^3)$ with $N_{unk} \geq 32$ (number of real unknowns). If an exhaustive search is applied, the complexity order is $\mathcal{O}(N_q^8)$ with N_q being the number of quantization levels.
- For the case of MISO user channel, the complexity for Eve could scale exponentially as the number of antennas on Alice increases.

Final Remarks

- While some details of RRCM for SISO user channel have been presented in these slides, also shown in this paper are the RRCM schemes for SIMO, MISO and SISO OFDM user channels.
- Further analytical results of the computational complexity needed for Eve to break the RRCM schemes will be shown in an upcoming paper.
- RRCM is a physical layer encryption method that exploits the abundance of bandwidth in future networks.
- The pros and cons of “physical layer encryption” versus “network layer encryption” deserve more investigations.

References Mentioned in the Slides

1. H. V. Poor and R. F. Schaefer, “Wireless physical layer security”, PNAS, Vol. 114, no. 1, pp.19-26, January 3, 2017.
2. Y.-K. Chia and A. El Gamal, “Wiretap channel with causal state information,” IEEE Transactions on Information Theory, Vol. 58, No. 5, pp. 2838-2849, May 2012.
3. T. R. Dean and A. J. Goldsmith, “Physical-layer cryptography through massive MIMO,” IEEE Transactions on Information Theory, Vol. 63, No. 8, pp. 5419-5436, Aug. 2017.
4. Y. Hua, “Advanced properties of full-duplex radio for securing wireless network”, IEEE Transactions on Signal Processing, pp. 120-135, Jan 1, 2019.

Thank You!