Physical Layer Security in Wireless Communications

Dr. Zheng Chang
Department of Mathematical Information Technology
zheng.chang@jyu.fi

Outline

- Fundamentals of Physical Layer Security (PLS)
- Coding for PLS
- Signal Processing for PLS
- Cooperation Communications for PLS
- Game theory for PLS
- Other advances in PLS

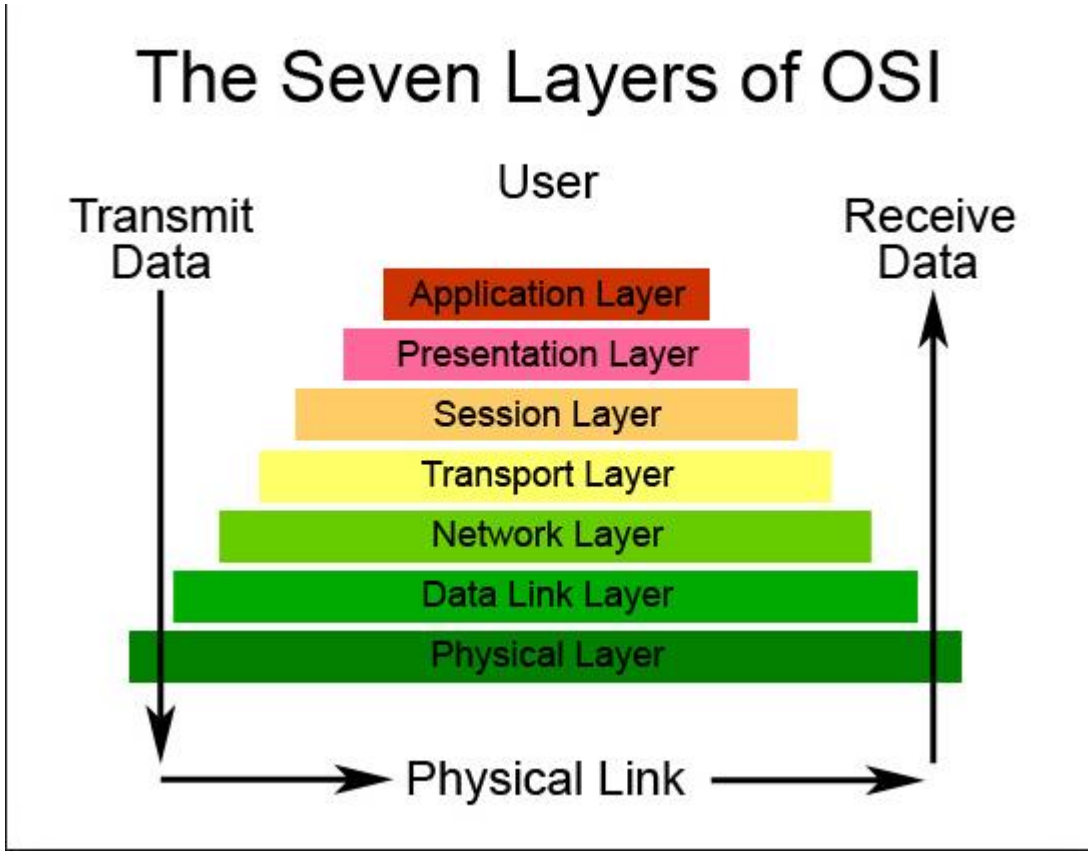
FUNDAMENTALS OF PHYSICAL LAYER SECURITY

Fundamentals of physical layer security
Physical Layer

- In the 7-layer Open System Interconnect (OSI) model of computer networking, the physical layer or layer 1 is the first (lowest) layer. It is commonly abbreviated PHY.
- The name “physical layer” can be a bit problematic. Many people who study networking get the impression that the physical layer is only about actual network hardware.
- PHY contains
  - Definition of Hardware Specifications
  - Encoding and Signaling
  - Data Transmission and Reception
  - Topology and Physical Network Design

Fundamentals of physical layer security

Physical Layer



Fundamentals of physical layer security
Physical Layer

- Some key tech in PHY
  - CDMA
  - OFDM
  - MIMO
  - …

Fundamentals of physical layer security
Physical Layer

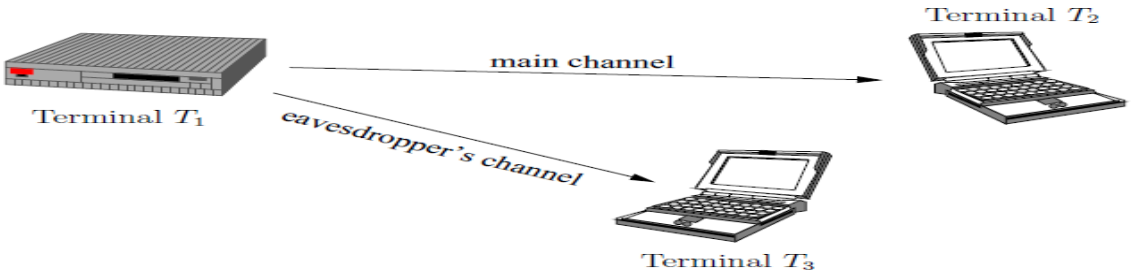
- In all communication systems, the issues of authentication, confidentiality, and privacy are handled in the upper layers of the protocol stack using variations of private-key and public-key cryptosystems.
- Nowadays, many results from information theory, signal processing, and cryptography suggest that there is much security to be gained by accounting for the imperfections of the physical layer when designing secure systems.

Fundamentals of physical layer security
Physical Layer

- For example, while noise and fading are usually treated as impairments in wireless communications, information-theoretic results show that they can be harnessed to “hide” messages from a potential eavesdropper or authenticate devices, without requiring a additional secret key.
- Such results, if they can be implemented in a cost-efficient way without sacrificing much data rate, call for the design of security solutions at the physical layer to complement communications security mechanisms.

Fundamentals of physical layer security

General Concept of PLS



The communication between terminals T1 and T2 is being eavesdropped by an unauthorized terminal T3. When terminals T2 and T3 are not collocated, radiofrequency signals observed at the outputs of the main channel and eavesdropper's channel are usually different. Natural discrepancies are caused by physical phenomena, and for wireless communications, the most notable effects are fading and path-loss. For instance, if T1 broadcasts a video stream, the signal obtained by T3 may be significantly degraded compared to the one received by T2; this degradation can even prevent T3 from understanding the content of the video stream.

Fundamentals of physical layer security

General Concept of PLS

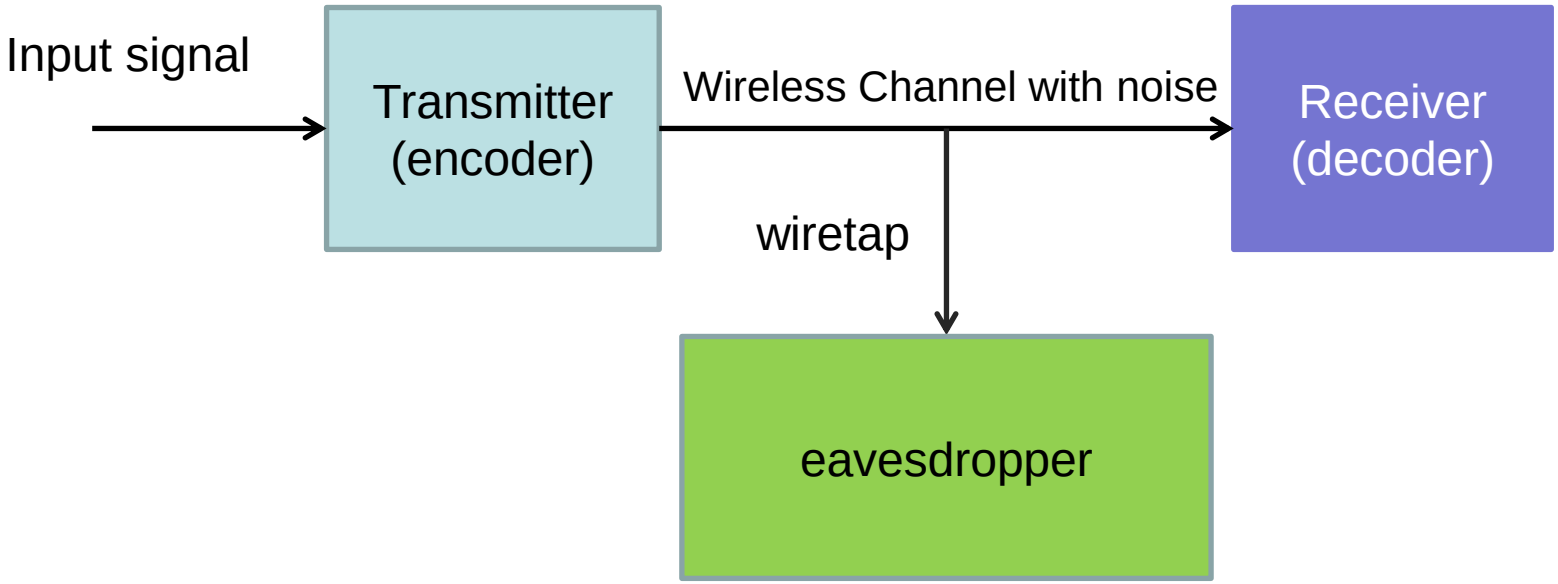


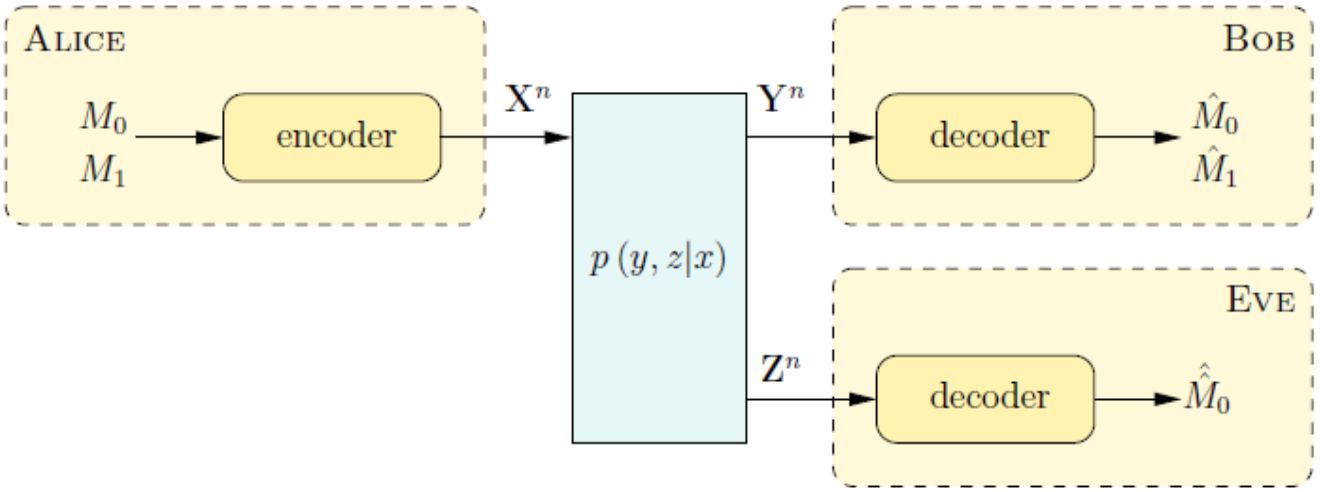
Fig. 1 Wiretap channel model

Fundamentals of physical layer security
General Concept of PLS

- The common secure communication framework does not account for the physical reality of communication channels.
- Especially, it does not consider the degradation of signals because of noise or fading.
- This observation naturally leads to the introduction of a more realistic communication model, now known as the wiretap channel, where noise in the main channel and eavesdropper's channel is explicitly introduced.

Fundamentals of physical layer security

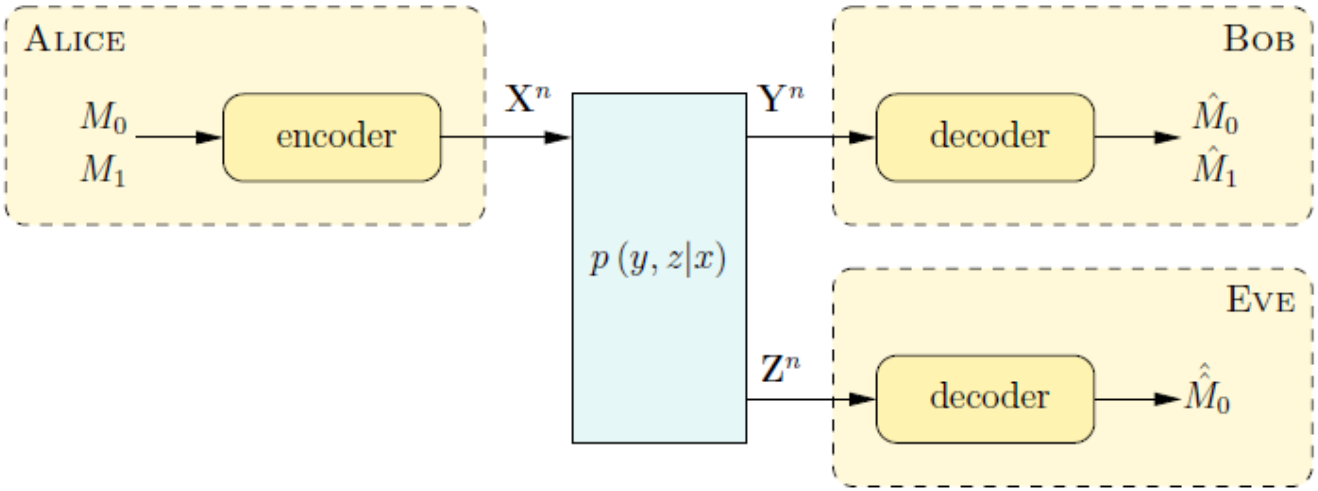
Wiretap Channel



It is also assumed that Alice wishes to send a common message M0 to both Bob and Eve and a private message M1 to Bob only. In the PLS, the common objective is to maximize the the secrecy capacity, which is usually defined as the data rate of confidential messages.

Fundamentals of physical layer security

Wiretap Channel

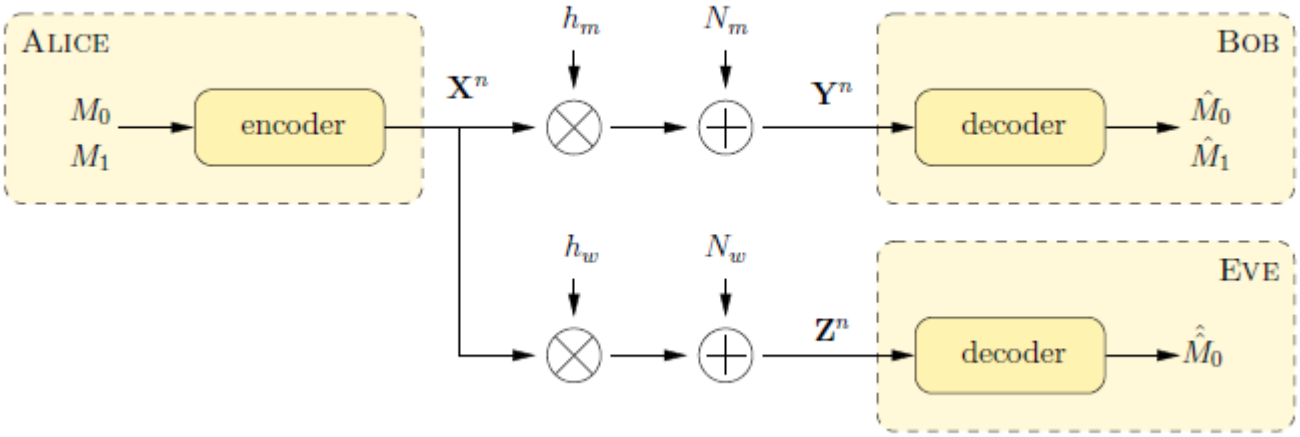


Essentially,

1. Z should provide no information about M1
2. Y can be decoded into M with negligibly small probability of error

Fundamentals of physical layer security

Wiretap Channel



Secrecy Capacity of Gaussian Wiretap Channel

$$C_s = \begin{cases} \frac{1}{2}\log_2\left(1+\frac{h_m^2 P}{\sigma_m^2}\right) - \frac{1}{2}\log_2\left(1+\frac{h_w^2 P}{\sigma_w^2}\right) & \text{if } \frac{h_m^2 P}{\sigma_m^2} > \frac{h_w^2 P}{\sigma_w^2}, \\ 0 \quad \text{otherwise.} \end{cases}$$

Fundamentals of physical layer security
Wiretap Channel

- To achieve security in PHY, there are multiple approaches,
  - Preprocessing Scheme
    - Coding
    - Key generation
    - Artificial Noise Scheme
  - Game Theortic Scheme
  - Signal Processing
  - Cooperation Communications
  - Many others

PREPROSSING FOR PLS

Preprocessing Scheme
Coding

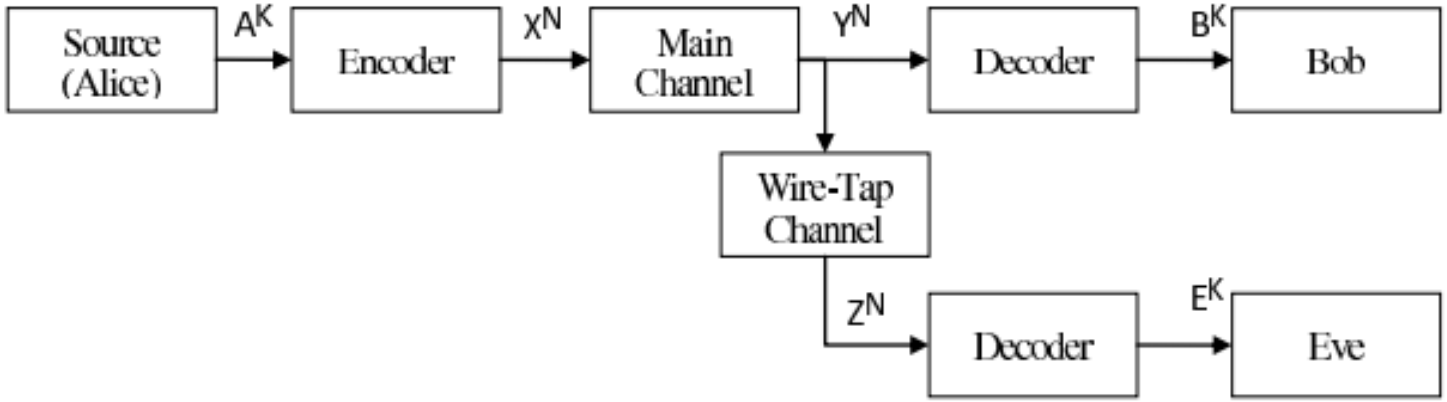
- Coding is a essential part in the wireless communications.

- In general, coding can be divided into two parts
  - Source Coding: modulation, typical: Morse code
  - Channel Coding: to protect information from transmission error.

- As the development of wireless communication technique, there are more types of coding, we can call it precoding which is usually used in MIMO , relay or some other systems.

Preprocessing Scheme
Coding

- With the introduction of the wiretap channel model, it became clear that security can also be achieved through means of channel coding.



Preprocessing Scheme
Coding

- The coding problem for Alice in the wire tap channel involves adding redundancy for enabling Bob to correct errors (across the main channel) and adding randomness for keeping Eve ignorant (across the wiretap channel), which is different from the coding in tranditional communications.

- Polar codes, LDPC can be used

- There are two types of coding approaches in general,
  - Capacity achieving based construction
  - Channel resolvability based construction

Preprocessing Scheme

Secure Key Generation

- To fully exploit the randomness of the channel for security purposes we need secrecy capacity-achieving channel codes.
- Unfortunately, it seems very difficult to design near-to-optimal codes for the Gaussian wiretap channel....
- Secret key agreement is a somewhat “easier” problem.
- Alice and Bob only have to agree on a key based on common randomness and not to transmit a particular message.

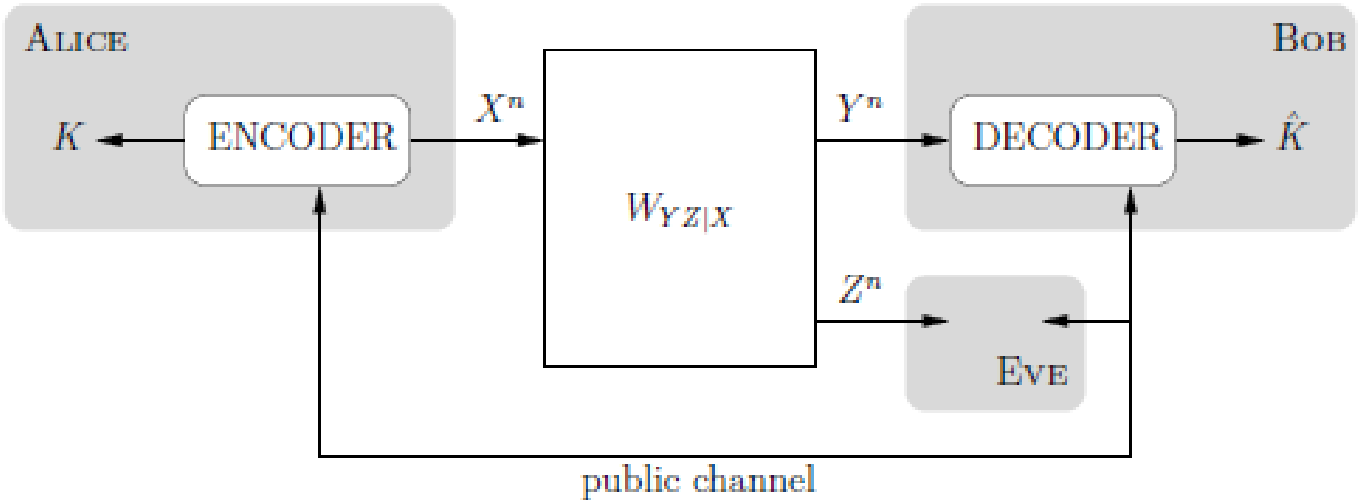
Preprocessing Scheme

Secure Key Generation

- This model is an extension of the wiretap channel.
- There exists a two-way, noiseless, public, side-channel of unlimited capacity.
- This model was introduced to analyze the effect of feedback on secret communications.
- The focus of this model is on the generation of secrecy from the channel in the form of secret keys.

Preprocessing Scheme

Secure Key Generation



Preprocessing Scheme

Secure Key Generation

- Alice and Bob can communicate over a public, authenticated, two-way side-channel of unlimited capacity.
- The assumption that the channel is public allows Eve to intercept all messages transmitted over the side-channel, so that the side-channel does not constitute a source of secrecy.
- However, the assumption that the channel is authenticated prevents Eve from tampering with the messages.

Preprocessing Scheme

Secure Key Generation

- The objective is for the legitimate parties Alice and Bob to exchange n symbols over the noisy channel and to transmit messages, collectively denoted by F, over the public channel, so that they eventually agree on the same secret key K unknown to Eve.
- A secret-key rate R is achievable if there exists a sequence of secret-key generation strategies with an increasing number of symbols transmitted over the noisy channels n, such that
  - The reliability requirement: with high probability, Alice and Bob agree on the same key.
  - The uniformity requirement: the secret key is uniformly distributed in its set, which is a desirable property if the key is to be used for cryptographic applications.
  - The secrecy requirement: the key is indeed secret with respect to Eve, who observes the noisy signals Zn and the public messages F.

Preprocessing Scheme

Secure Key Generation

- Alice and Bob can communicate over a public, authenticated, two-way side-channel of unlimited capacity.
- The assumption that the channel is public allows Eve to intercept all messages transmitted over the side-channel, so that the side-channel does not constitute a source of secrecy.
- However, the assumption that the channel is authenticated prevents Eve from tampering with the messages.

Preprocessing Scheme
Secure Key Generation

- The remarks :
  - The addition of a public authenticated channel does not trivialize the problem, because it is not a resource for secrecy. The only resource for secrecy remains the noisy communication channel.
  - Unlike the wiretap channel model, the channel model for secret-key generation allows for two-way communication and feedback. Feedback turns out to be an essential ingredient for secret-key generation. In addition, the key K is not a message in the traditional sense because its value needs to be fixed at the beginning of a secret-key generation strategy. This allows the key to be generated interactively based on the observations and messages of all legitimate parties, and to be processed with noninvertible functions. This contrasts with the wiretap channel model in which the secret message from the transmitter must be received unaltered.
  - Secret-key generation strategies can be extremely sophisticated

Preprocessing Scheme

Secure Key Generation

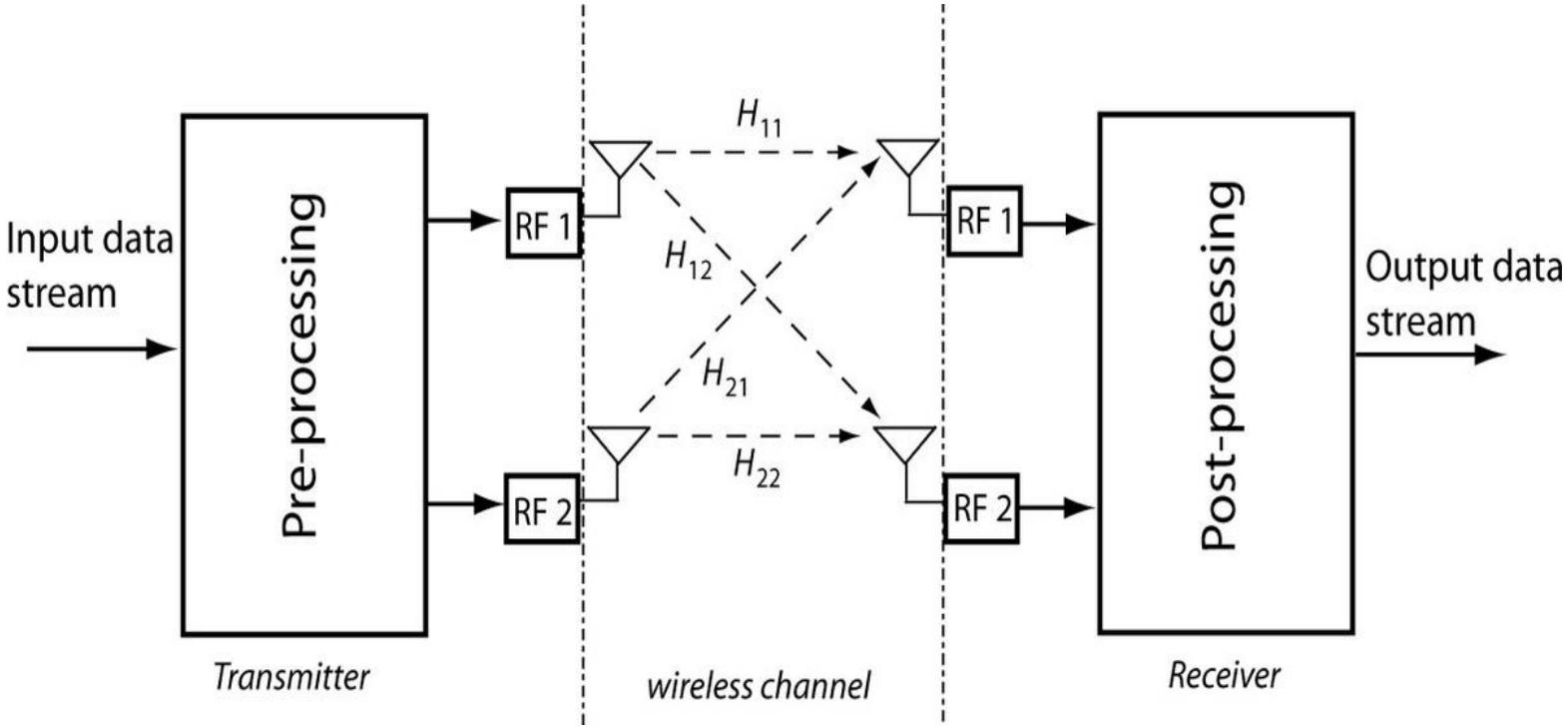
- There are some other possible ways to enhance the security at the transmitter side.
- For example, the Alice can artificially make some noise when transmitting the message.
- However, it requires Bob to correctly detect and estimate the information

SIGNAL PROCESSING FOR PLS

Signal processing for PLS

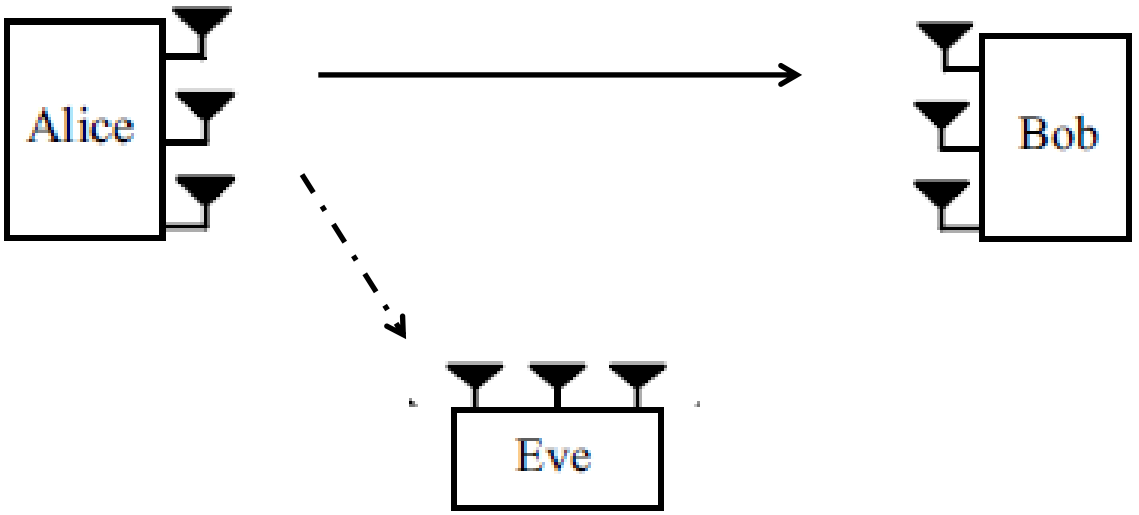
- The analysis of PLS frequently involve idealized assumptions of perfectly known global CSI, random coding arguments, Gaussian inputs, and so on.
- The signal processing perspective on physical layer security then naturally pertains to optimal and near-optimal transceiver design in situations where these assumptions may or may not hold.
- Two categories
  - PLS in MIMO
  - Channel estimation effect to PLS

Signal processing for PLS MIMO



P2P MIMO System

Signal processing for PLS MIMO



Signal processing for PLS MIMO

- A MIMO wiretap channel consists of a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve) equipped with N_T ,N_R, and N_E antennas, respectively. A general representation for the signal received by the legitimate receiver is

$$\mathbf{x}_a \in \mathbb{C}^{N_T \times 1}$$

$$\mathbf{y}_b = \mathbf{H}_b \mathbf{x}_a + \mathbf{n}_b, \qquad \mathbf{H}_b \in \mathbb{C}^{N_R \times N_T}$$

The received signal at the eavesdropper is

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x}_a + \mathbf{n}_e, \qquad \mathbf{H}_e \in \mathbb{C}^{N_E \times N_T}$$

Signal processing for PLS MIMO

$$C_s = \max_{\mathbf{Q}_x, \mathrm{Tr}(\mathbf{Q}_x) \leq P} \left[I\left(\mathbf{X}_a; \mathbf{Y}_b\right) - I\left(\mathbf{X}_a; \mathbf{Y}_e\right) \right]$$

$$C_s = \max_{\mathbf{Q}_x, \mathrm{Tr}(\mathbf{Q}_x) \leq P} \log\det\left(\mathbf{I} + \mathbf{H}_b \mathbf{Q}_x \mathbf{H}_b^H\right) - \log\det\left(\mathbf{I} + \mathbf{H}_e \mathbf{Q}_x \mathbf{H}_e^H\right),$$

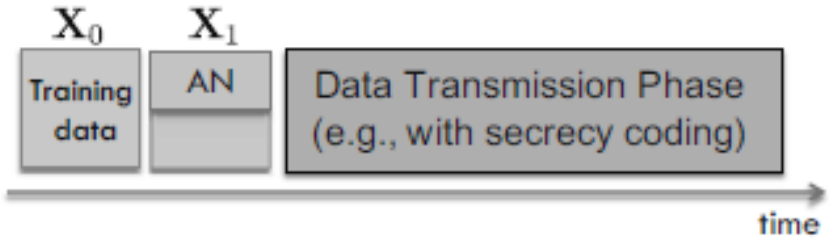
Signal processing for PLS MIMO

- Although, the mathematical formulation seems no difference between the SISO and MIMO structure, due to the complexity of MIMO system, there are many additional schemes can be applied.
- For example, precoding for MIMO, MIMO interference effect, channel matrix etc.

Signal processing for PLS
Channel Estimation

- The PLS can be enhanced through signal processing technology.
- Here, we briefly overview one typical channel estimation scheme, of which a key feature is the insertion of artificial noise (AN) in the training signal to degrade the channel estimation performance at Eve. To do so, AN must be placed in a carefully chosen subspace to minimize its effect on Bob.
- However, this requires preliminary knowledge of the channel at the Alice, which can be difficult to achieve without benefiting the channel estimation at Eve as well.
- Therefore, advanced training scheme should be investigated.

Signal processing for PLS
Channel Estimation



Two-Stage Feedback-and-Retraining

- In the initial stage, the transmitter first emits a sequence of training signals (that consists of only pilot signals) for preliminary channel estimation at Bob.
- In this stage, Bob sends back channel state to he Alice, who utilizes this information to determine the AN placement in the training signal. Please note that Eve is also allowed to intercept the feedback sent by Bob but, as can be seen later on, this information does not help UR improve the channel estimate of its own channel.

Signal processing for PLS
Summary

- The signal processing technique contains many different aspects.
- In addition to aforementioned schemes, there are some other schemes that can improve the PLS performance.
- For example, the transceiver design, modulation, beamforming in MIMO etc.

COOPERATION COMMUNICATIONS FOR PLS

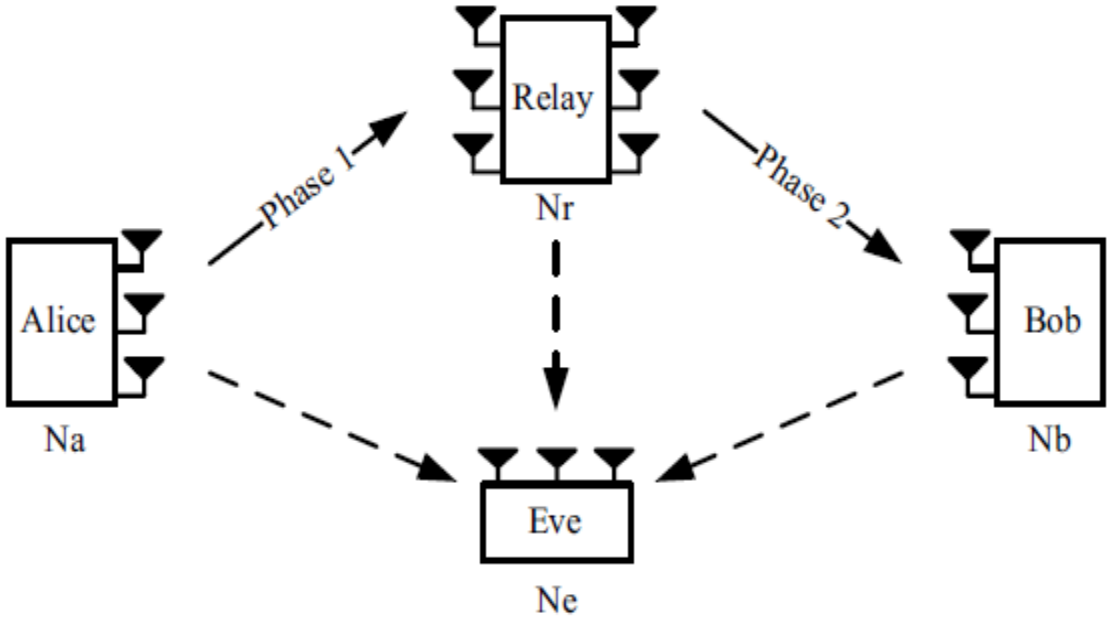
Cooperation Communications for PLS

- There are many ways to explore the coopration in wireless communications.
  - Relay
  - User cooperation
  - BS cooperation
- For relay network, security issues are very important as extra entities are involved during transmission.
- We first introduce some prelimary of relay

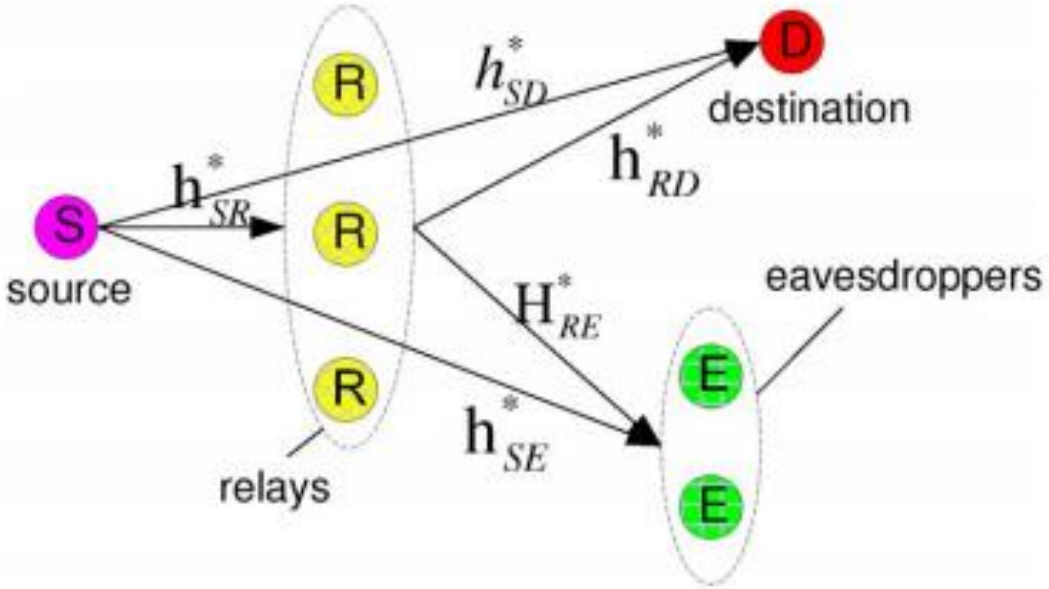
Cooperation Communications for PLS

- By mobilty
  - Fixed relay
  - Mobile relay
- By processing technique
  - Amplified-and-Forward
  - Decode-and-Forward

Cooperation Communications for PLS



Cooperation Communications for PLS



$$R_s = \max\{R_d - R_e\}$$

Cooperation Communications for PLS

- Some key features
  - Cooperative Jamming
  - Relay Chatting

different to cooperative jamming, the success of relay chatting relies on the selection of relaying and jamming nodes. Specifically a node is selected to transmit jamming information only if its connection to the legitimate receivers is poor

Cooperation Communications for PLS

- There are many critical issues involved,
  - How many relays should be selected
  - Which relay should be selected
  - Which types of relays should be used.
  - How the channel should be modelled.
  - Whether the Channel state information is known
  - Whether the relay is trustful.

Cooperation Communications for PLS

- Here we mainly elaborate the relay transmission .
- Also there are many other cooperation mechenisms.
  - User cooperation
  - BS cooperation

GAME THEORY FOR PLS

Game Theory for PLS

- Whats game theory?
  - Game theory is a study of strategic decision making. Specifically, it is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers". An alternative term suggested "as a more descriptive name for the discipline" is interactive decision theory.

Game Theory for PLS

- The normal (or strategic form) game is usually represented by a matrix which shows the players, strategies, and payoffs.
- The classic prisoners' dilemma

Pareto optimal

	Prisoner B stays silent (*cooperates*)	**Prisoner B betrays (*defects*)**
Prisoner A stays silent (*cooperates*)	Each serves 1 year	Prisoner A: 3 years Prisoner B: goes free
Prisoner A betrays (*defects*)	Prisoner A: goes free Prisoner B: 3 years	Each serves 2 years

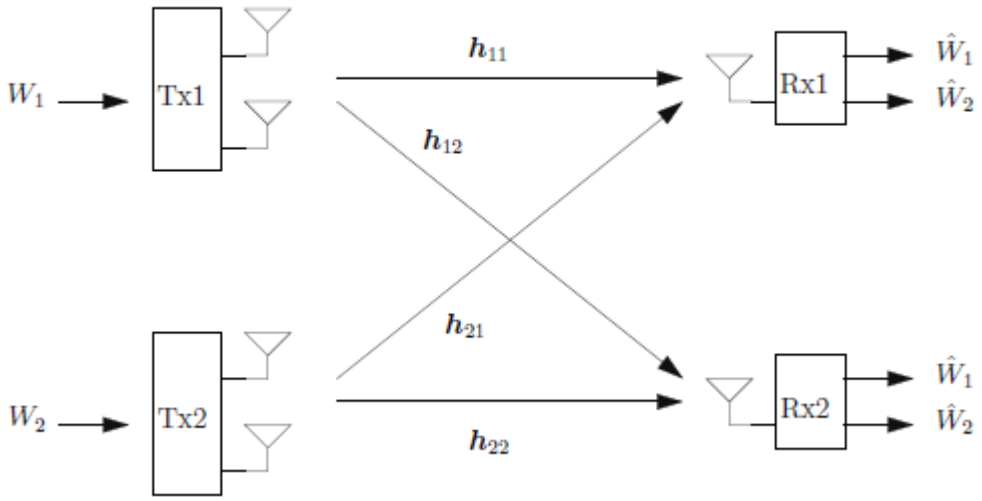
Nash equilibrium

Game Theory for PLS

- There are two kinds of games, noncooperative game and cooperative game.
  - a **non-cooperative game** is one in which players make decisions independently.
  - a **cooperative game** is a game where groups of players ("coalitions") may enforce cooperative behaviour.

The application of game theory to PLS is to find reasonable efficient operating points for wireless communications systems under secrecy constraints. We use a example to briefly explain the application of game theory to PLS.

Game Theory for PLS



We consider a MISO interference channel, where two transmitters have multiple antennas and the receivers has single antenna.

Game Theory for PLS
case 1: all public

- The messages by both links are public, but receiver 1 is only interested in the message from transmitter 1, and receiver 2 only in message from transmitter 2, respectively.

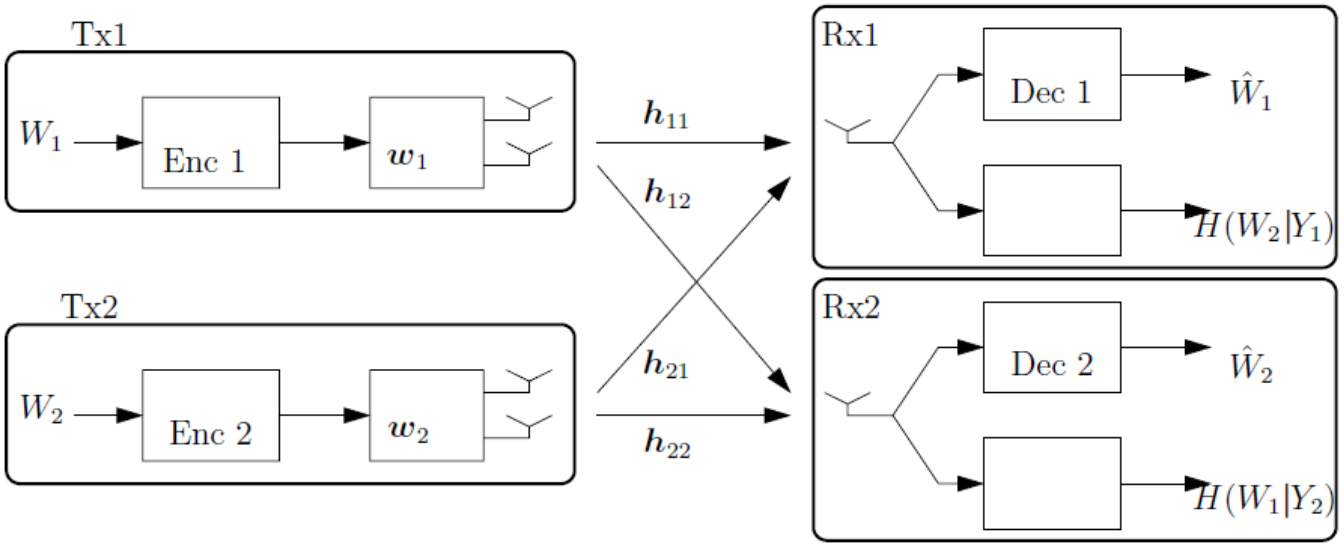
- In this case, the aim is to maximize the data rate of individual link,

$$R_1(\boldsymbol{w}_1, \boldsymbol{w}_2) = \log\left(1 + \frac{|\boldsymbol{w}_1^H \boldsymbol{h}_{11}|^2}{\sigma_n^2 + |\boldsymbol{w}_2^H \boldsymbol{h}_{21}|^2}\right)$$

$$R_2(\boldsymbol{w}_1, \boldsymbol{w}_2) = \log\left(1 + \frac{|\boldsymbol{w}_2^H \boldsymbol{h}_{22}|^2}{\sigma_n^2 + |\boldsymbol{w}_1^H \boldsymbol{h}_{12}|^2}\right).$$

Game Theory for PLS
case 2: all private

- Now, the two messages are private and intended only for the corresponding receivers.



Game Theory for PLS

case 2: all private

Securecy rate

$$
\begin{aligned}
{}_sR_1 &= \underbrace{\log\left(1+\frac{\rho|\boldsymbol{w}_1^H\boldsymbol{h}_{11}|^2}{1+\rho|\boldsymbol{w}_2^H\boldsymbol{h}_{21}|^2}\right)}_{\text{information term}} - \underbrace{\log\left(1+\rho|\boldsymbol{w}_1^H\boldsymbol{h}_{12}|^2\right)}_{\text{secrecy term}} \\
{}_sR_2 &= \log\left(1+\frac{\rho|\boldsymbol{w}_2^H\boldsymbol{h}_{22}|^2}{1+\rho|\boldsymbol{w}_1^H\boldsymbol{h}_{12}|^2}\right) - \log\left(1+\rho|\boldsymbol{w}_2^H\boldsymbol{h}_{21}|^2\right).
\end{aligned}
$$

Achievable secrecy rate region

$$
{}_s\mathcal{R} = \bigcup \{{}_sR_1, {}_sR_2\}.
$$

OTHER ADVANCES

Some other issues

- Stochastic Geometry Approaches
- PLS in OFDMA Networks
- Multihop security

Stochastic Geometry Approaches

- Stochastic geometry can be applied to study the physical layer security performance, especially in the large-scale wireless networks.
- Legitimate users and the eavesdroppers are randomly located over a large geographical area according to some probability distributions.
- There are some interesting study points.
  - The secrecy graph, as a graph-theoretic approach, is introduced to study the connectivity properties among the legitimate users of the network. It characterizes the existence of connection with perfect secrecy between any two legitimate users.
  - The secrecy transmission capacity. It considers concurrent transmissions between all the legitimate links and gives a mathematically tractable measure on the achievable network throughput with a given secrecy requirement.

Stochastic Geometry Approaches

- The simplest yet most important model in Stochastic Geometry is the homogenous Poisson point process (PPP). A homogenous PPP in an n-dimensional (usually two-dimensional) space roughly means that all nodes are randomly located inside the network according to a uniform distribution.
- It is completely characterized by the constant intensity parameter λ. Specifically, the value of λ gives the average number of nodes located inside a unit volume in the n-dimensional space.

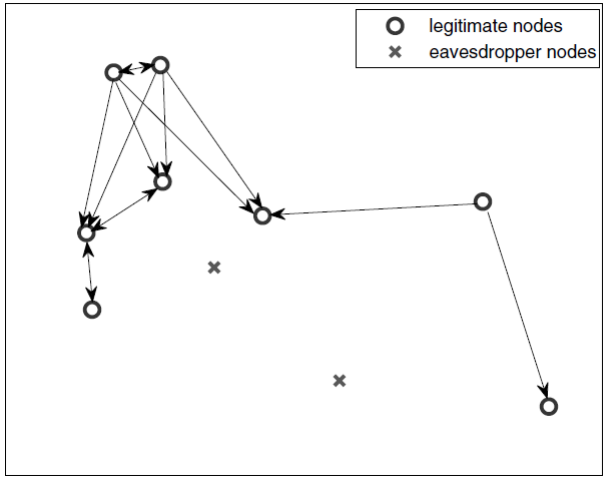
- By such stochastic geometry modelling, we are able to solve the problem in the large scale wireless networks.

Stochastic Geometry Approaches

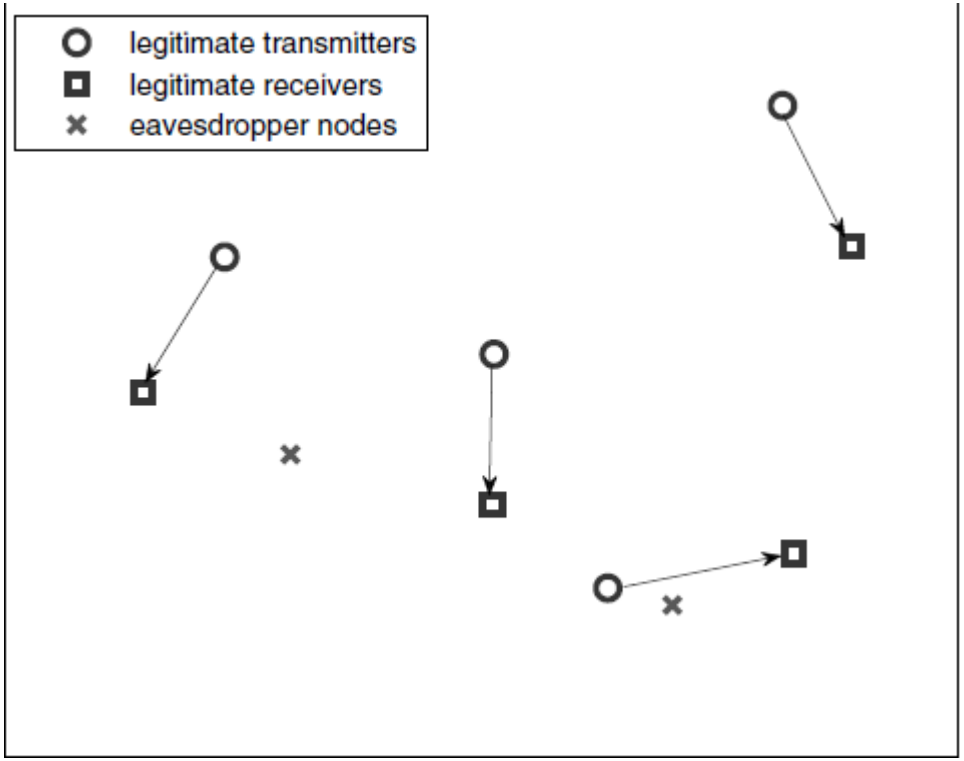
- We have discussed the transmission capacity in a P2P manner.
- Secrecy Transmission Capacity
  - The basic idea behind the stochastic geometry approach is as follows: although it is extremely difficult to directly characterize the throughput performance limit of a network, it is often tractable to study the performance of a typical communication pair, taking into account the interaction from other nodes in the network.
  - Furthermore, if all nodes have roughly the same properties, e.g., transmit power, code rate, mobility, etc., then the average performance of the typical communication pair represents the average performance of all the links in the network.

Stochastic Geometry Approaches

- Secrecy Graph
  - In decentralized networks, communication is usually initiated in an ad hoc manner with loose or completely random medium access control (MAC). The message transmitted from a source to a destination requires multiple intermediate relays when the source and destination are separated by a large distance. Therefore, a high level of connectivity becomes a very important prerequisite for reliable communications over the entire network.
  - Whether there exists a secure communication link between any two legitimate nodes depends not only on the locations and channel quality of these two nodes, but also on the locations and channel qualities of all the eavesdroppers.



Stochastic Geometry Approaches



Stochastic Geometry Approaches

- Connection Outage: The event that the capacity of the channel from the transmitter fo the intended receiver is below the codeword rate Rt. The probability of this event happening is referred to as the connection outage probability, denoted by Pco.
- Secrecy Outage: The event that the capacity of the channel from the transmitter to at least one eavesdropper is above the rate redundancy Re. The probability of this event happening is referred to as the secrecy outage probability, denoted by Pso.

Stochastic Geometry Approaches

- Let us consider a decentralized wireless network in a two-dimensional space. Homogeneous PPPs are used to model the locations of both the legitimate nodes and the eavesdroppers. Specifically, the locations of the legitimate transmitters follow a homogeneous PPP, with intensity λ_l. Each transmitter has an intended receiver at a fixed distance r in a random direction. Then the secrecy transmission capacity

Pco

$$\tau = R_s(1-\bar{\sigma})\lambda_l.$$

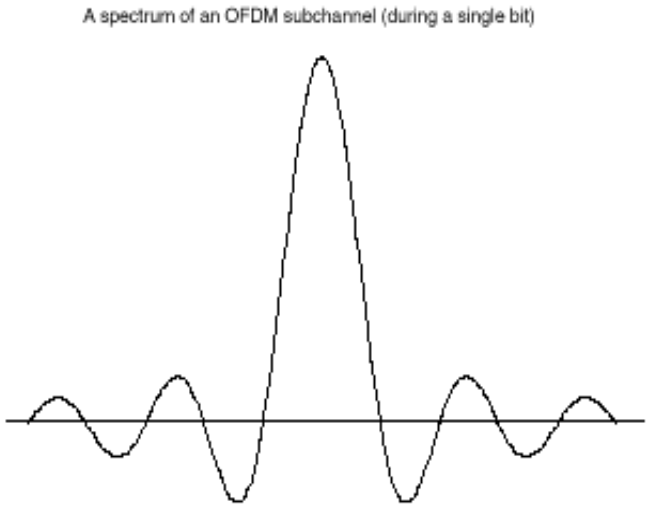
the confidential data rate

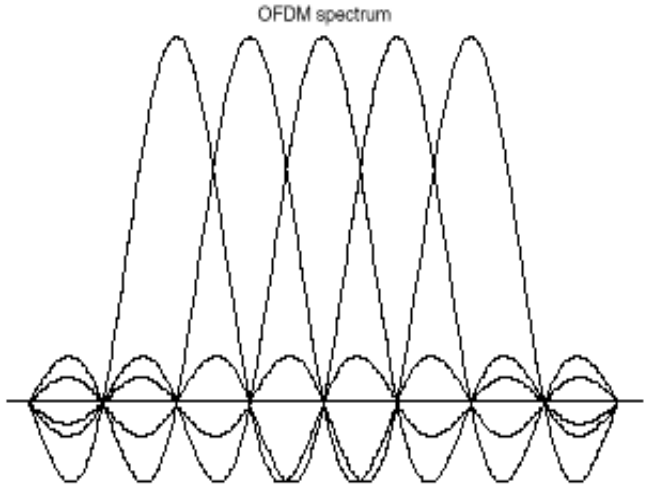
PLS in OFDMA Networks

- OFDMA is the physical layer technique used in the current 4G networks, WiFi networks and many other.

- OFDM is a frequency-division multiplexing (FDM) scheme used as a digital multi-carrier modulation method. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channels. Each sub-carrier is modulated with a conventional modulation scheme (such as quadrature amplitude modulation or phase-shift keying) at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

PLS in OFDMA Networks



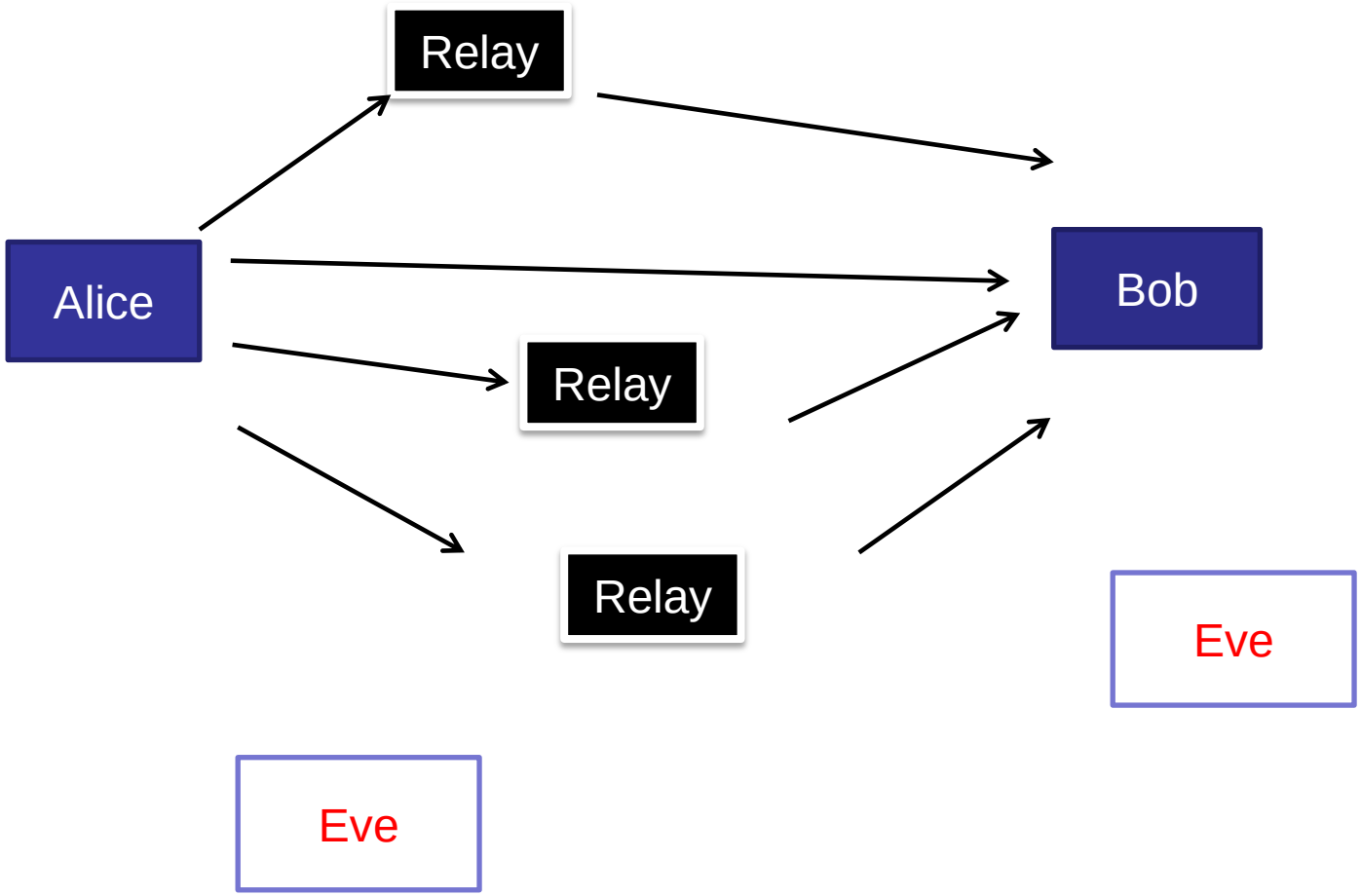


PLS in OFDMA Networks

- So for the PLS in OFDMA networks, the focus is to design the related methods to ehance the security.
- The security is usually measured by securecy data rate/capacity, outage probabilities etc.
- Whats make OFDMA different from other technique is the use of number of subcarriers.
- Therefore, subcarrier allocation scheme is the main focus in this area.

PLS in OFDMA Networks

how the schedule the transmission subcarrier in this case?



THANKS