Physical Layer Security Techniques

Yaru Fu

Assistant Professor
School of Science and Technology (S&T)
Hong Kong Metropolitan University (HKMU)

Apr. 2022

Commonly Used PLS Techniques in the Research Community

- 1. Artificial Noise Generation
- 2. Multi-Antenna Diversity
- 3. Multi-User Diversity
- 4. Cooperative Diversity

1. Artificial Noise Generation

The main idea of this technique is to artificially degrade Eve's channel by injecting artificial noise (AN). The process consists in that an authorized node in the network (e.g., Alice, Bob, or another) adds well designed artificially jamming signals to the transmitted signal that can only harm Eve's channel. The basic system model of AN network for PLS is depicted in Fig. 1.

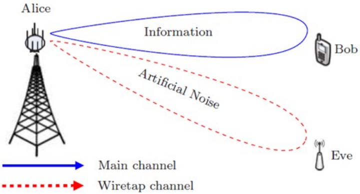
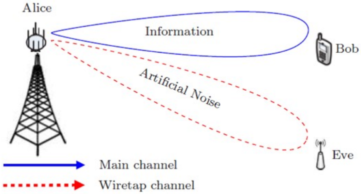


Figure 1: The model of AN network for a wiretap channel consisting of two main nodes and an eavesdropper

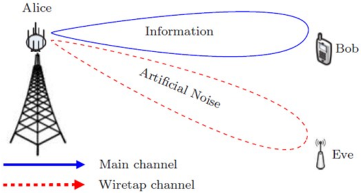
1. Artificial Noise Generation

- We consider that the transmitter (A) has N_A antennas ($N_A > 1$) and the receiver (B) has a single antenna. This scenario is representative, particularly for the downlink transmission in cellular systems.
- Eavesdroppers (E) is assumed to individually overhear the communication between A and B
- We denote the channel between A and B and the channel between A and E as $\boldsymbol{h}$ and $\boldsymbol{g}$, respectively
- The knowledge of $\boldsymbol{h}$ can be obtained at A either from uplink (or reverse) training if channel reciprocity holds or using a feedback link from B to A
- We assume the knowledge of both $\boldsymbol{h}$ and $\boldsymbol{g}$ are known at A



1. Artificial Noise Generation

- The key idea of guaranteeing secure communication using artificial noise proposed is described as follows. The transmitter utilizes multiple antennas to transmit the information bearing signal into the receiver's channel, at the same time generating a noise-like signal into the null space of the receiver's channel



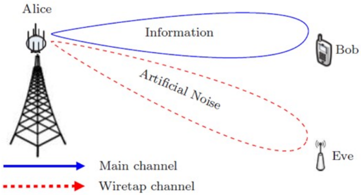
1. Artificial Noise Generation

- Let $\boldsymbol{W} = [\boldsymbol{w}_1, \boldsymbol{W}_2]$, where $\boldsymbol{w}_1 = \boldsymbol{h}^* / ||\boldsymbol{h}||$, which can be taken as the beamforming vector for transmitting the signal to Bob.
- The transmit signal at Alice is $\boldsymbol{x} = \boldsymbol{w}_1 u + \boldsymbol{W}_2 \boldsymbol{v}$
- Therefore, the received symbols at B and E are given by, respectively,

$$y_B = \boldsymbol{h}\boldsymbol{x} + n = \boldsymbol{h}(\boldsymbol{w}_1 u + \boldsymbol{W}_2 \boldsymbol{v}) + n = ||\boldsymbol{h}|| u + n \tag{1}$$

$$y_E = \boldsymbol{g}\boldsymbol{x} + e = \boldsymbol{g}(\boldsymbol{w}_1 u + \boldsymbol{W}_2 \boldsymbol{v})\boldsymbol{h} + e = \boldsymbol{g}\boldsymbol{w}_1 u + \boldsymbol{g}\boldsymbol{W}_2 \boldsymbol{v} + e, \tag{2}$$

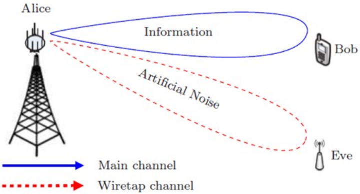
where n and e are the additive white Gaussiaen noises (AWGN) at B and E.



We see in (1) that $\boldsymbol{W}_2$ spans the null space of $\boldsymbol{h}$, hence the artificial noise $\boldsymbol{v}$ does not affect the received signal at B

1. Artificial Noise Generation

- Power allocation at Alice, P_A
- Channel estimate
- Extent to Multiple users scenario



2. Multi-Antenna Diversity

- All the network nodes are equipped with multiple antennas
- As is known, multiple input and multiple output (MIMO) has been shown as an effective means to combat wireless fading and increase the capacity of wireless channel. However, the eavesdropper can also exploit the MIMO structure to enlarge the capacity of wiretap channel from source to eavesdropper.
- Thus, without a proper design, it may fail to increase the secrecy capacity of wireless transmission with MIMO.
  - For example, if the conventional open-loop space-time block coding is considered, the destination should first estimate the main channel matrix $\boldsymbol{h}_B$ and then perform the space-time decoding process with an estimated $\hat{\boldsymbol{h}}_B$, leading the diversity gain to be achieved for the main channel. Similarly, the Eve can also estimate the wiretap channel matrix $\boldsymbol{h}_E$ and then conduct the corresponding space-time decoding algorithm to obtain diversity.

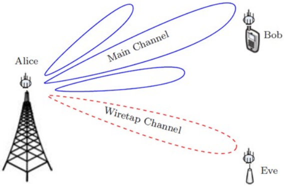
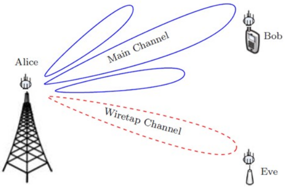


Figure 2: A MIMO wireless system by using secure beamforming with nulls directed towards Eve

2. Multi-Antenna Diversity

- Generally speaking, if the source node transmits its signal to the desired destination with N_A antennas, Eve will also receive N_A signal copies for interception purposes. In order to defend against eavesdropping attacks, the source node should adopt a preprocess that needs to be adapted to the main and wiretap channels $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$ such that the diversity gain can be achieved at destination only whereas the eavesdropper benefits nothing from the multiple transmit antennas at source.

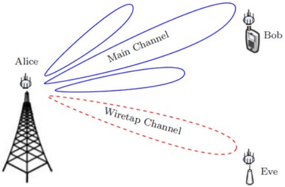
- Ideally, the objective of such preprocess (adaptive transmit process) is to maximize the secrecy capacity of MIMO transmission, which, however, requires the channel state information (CSI) of both main and wiretap links (i.e., $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$). In practice, the wiretap channel information $\boldsymbol{h}_E$ may be unavailable, since the eavesdropper is usually passive and keeps silent.
  - If only the main channel information $\boldsymbol{h}_B$ is known, the preprocess can be designed to maximize the main channel capacity, which does not require the knowledge of wiretap channel $\boldsymbol{h}_E$.
  - Since the adaptive transmit process is optimized based on the main channel information $\boldsymbol{h}_B$ and the wiretap channel is typically independent of the main channel, the main channel capacity will be significantly increased with MIMO and no improvement will be achieved for the wiretap channel capacity.



2. Multi-Antenna Diversity

Three preprocess manners:

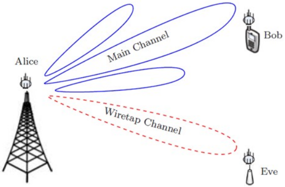
- 1). Transmit beamforming: this is a signal processing technique by combining multiple transmit antennas at the source node in such a way that desired signals transmit in a particular direction to destination
  - Considering that Eve and Bob generally lie in different directions relative to the source node, the desired signals (with transmit beamforming) that are received at Eve will experience destructive interference and become very weak. Thus, the transmit beamforming is effective to defend against eavesdropping attacks when the destination and eavesdropper are spatially separated.



2. Multi-Antenna Diversity

Three preprocess manners:

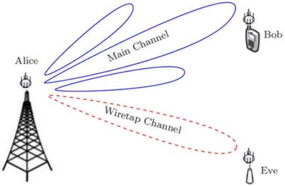
- 2). Power allocation: The power allocation is to maximize the main channel capacity (or secrecy capacity if both $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$ are known) by allocating the transmit power among N_A antennas at source.
  - In this way, the secrecy capacity of MIMO transmission will be significantly increased, showing the security benefits of using power allocation against eavesdropping attacks.



2. Multi-Antenna Diversity

Three preprocess manners:

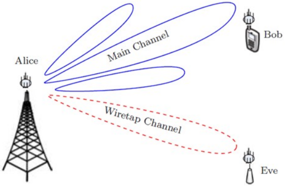
- 3). Transmit antenna selection: Depending on whether the global CSI of main and wiretap channels (i.e., $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$) is available, an optimal transmit antenna at the source node will be selected and used to transmit source signals.
  - If both $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$ are available, a transmit antenna with the highest secrecy capacity will be chosen
  - If only $\boldsymbol{h}_B$ is known, the transmit antenna selection is to maximize the main channel capacity



2. Multi-Antenna Diversity

Summary:

- One can observe that the above mentioned three approaches (i.e., transmit beamforming, power allocation, and transmit antenna selection) all have great potential to improve the physical-layer security of MIMO wireless systems against eavesdropping attacks.
  - by maximizing secrecy capacity with the information of $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$
  - by maximizing the main channel capacity with the information of $\boldsymbol{h}_B$



3. Multi-user Diversity

System Model

- A base station (BS) serves multiple users where M users, denoted by $U_1, \ldots, U_M$.
- In cellular networks, M users typically communicate with BS with an orthogonal multiple access mechanism such as the orthogonal frequency division multiple access (OFDMA) and time division multiple access (TDMA). Taking the OFDMA as an example, the OFDM subcarriers are allocated to different users. In other words, given an OFDM subcarrier, we need to determine which user should be assigned to access and use the subcarrier for data transmission.

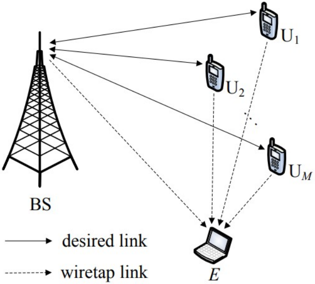


Figure 3: A multiuser wireless communications system consisting of one base station (BS) and multiple users in the presence of an eavesdropper

3. Multi-User Diversity

System Model

- Traditionally, a user with the highest throughput is selected to access the given OFDM subcarrier, aiming at maximizing the transmission capacity.
- This relies on the knowledge of main channel information only and can provide the significant multiuser diversity gain

  for performance improvement
  - if a user is far away from BS and experiences severe propagation loss and deep fading, it may have no chance to be selected as the "best" user for channel access. To this end, user fairness should be further considered in the multiuser scheduling, where two competing interests need to be balanced: maximizing the main channel capacity while at the same time guaranteeing each user with certain opportunities to access the channel.
- With the multiuser scheduling, a user is first selected to access a channel (i.e., an OFDM subcarrier in OFDMA or a time slot in TDMA) and then starts transmitting its signal to BS. Meanwhile, due to the broadcast nature of wireless transmission, the eavesdropper overhears such transmission and attempts to interpret the source signal

3. Multi-User Diversity

How PLS is performed?

- In order to effectively defend against the eavesdropping attack, the multiuser scheduling should be performed to minimize the wiretap channel capacity while maximizing the main channel capacity, which requires the CSI of both main and wiretap links.
  - If only the main channel information is available, we may consider the use of conventional multiuser scheduling.
- It needs to be pointed out the conventional multiuser scheduling still has great potential to enhance the physical-layer security, since the main channel capacity is significantly improved with conventional multiuser scheduling while the wiretap channel capacity remains the same.

4. Cooperative Diversity

Cooperative Communication:

- Cooperative communications is used to provide reliability and extended coverage
- Two types of relay
  - amplify and forward (AF): In the AF protocol, a relay node simply amplifies and retransmits its received noisy version of the source signal to the destination
  - decode and forward (DF): In contrast, the DF protocol requires the relay node to decode its received signal and forward its decoded outcome to the destination node

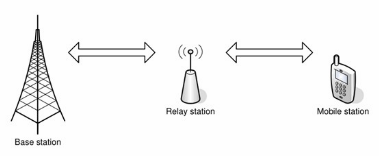


Figure 4: An illustration of cooperative communication

4. Cooperative Diversity

- Cooperative communications, which, besides providing reliability and extended coverage, are used for improving the PLS performance.
- Relaying techniques allow the transmitter sends its information to the destination through a relay located between the two nodes.

- Relays can be configured in different ways to counteract eavesdropping.
  - they can behave like a conventional relay to attend the legitimate communication (Fig. 5a)
  - they can also act as jammers by sending AN to degrade Eve's channel
  - they can also take the role of potential eavesdroppers when they are untrusted, i.e., the confidential signals are vulnerable (Fig. 5b)

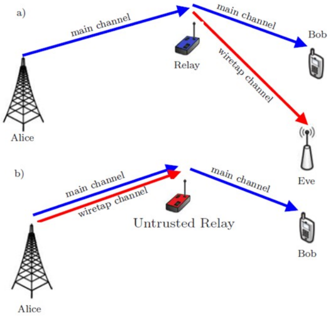
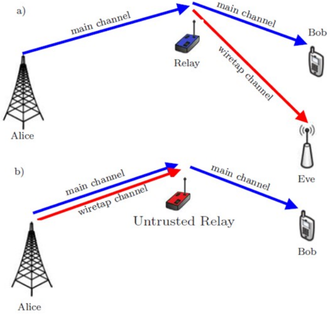


Figure 5: a) Traditional relay network in wiretap channel. b) Untrusted relay network in wiretap channel

4. Cooperative Diversity

1) Cooperative Relaying Methods to Provide PLS: one single relay

- DF
- AF
- Cooperative jamming



4. Cooperative Diversity

2) Cooperative Relaying Methods to Provide PLS: multiple relays

- Fig. 6 shows a cooperative wireless network including one source, M relays, and one destination in the presence of an eavesdropper, where M relays are exploited to assist the signal transmission from source to destination. To be specific, the source node first transmits its signal to M relays that then forward their received source signals to destination.

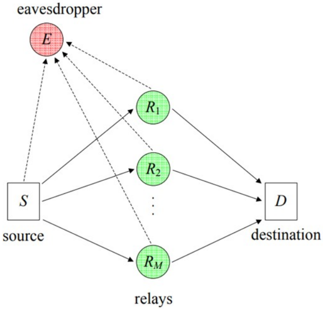


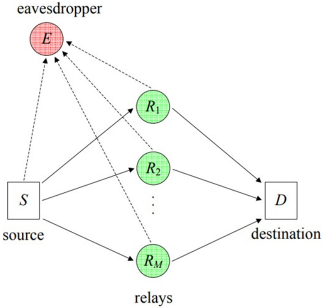
Figure 6: A cooperative diversity system consisting of one source, M relays, and one destination in the presence of an eavesdropper

4. Cooperative Diversity

2) Cooperative Relaying Methods to Provide PLS: multiple relays

Two manners:

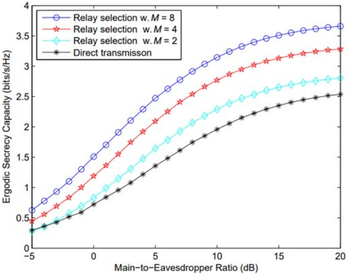
- Cooperative beamforming: multiple relays can form a virtual antenna array and cooperate with each other to perform transmit beamforming such that the signals received at the intended destination experience constructive interference while the others (received at eavesdropper) experience destructive interference
- The best relay selection: in the best relay selection, a relay node with the highest secrecy capacity (or highest main channel capacity if only the main channel information is available) is chosen to participate in assisting the signal transmission from source to destination



5. Some Numerical Results

1) Secrecy Capacity

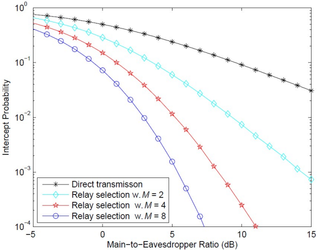
- secrecy capacity of best relay selection scheme is always higher than that of direct transmission, showing the wireless security benefits of using cooperative relays
- as the number of relays M increases from $M = 2$ to $M = 8$, the secrecy capacity of best relay selection scheme significantly increases, i.e., increasing the number of cooperative relays can improve the physical-layer security of wireless transmission against eavesdropping attacks.



5. Some Numerical Results

2) Intercept Probability

- the best relay selection scheme outperforms the conventional direct transmission in terms of intercept probability
- as the number of cooperative relays M increases from $M = 2$ to $M = 8$, the intercept probability improvement of best relay selection over direct transmission becomes much more significant


10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
Intercept Probability
Main−to−Eavesdropper Ratio (dB)
Direct transmisson
Relay selection w. M = 2
Relay selection w. M = 4
Relay selection w. M = 8