Physical Layer Security for Space Shift Keying (SSK) Transmission

Sina Rezaei Aghdam

under supervision of: Prof. Tolga M. Duman
Dept. of Electrical and Electronic Engineering, Bilkent University, Ankara, Turkey.
Physical Layer Security

• Securing the communications at the physical layer;
an alternative to the conventional higher network-layer solutions for security

• Basic principle:
to exploit the randomness of communications channels to allow a transmitter to
deliver its message to an intended receiver while guaranteeing that a third party
cannot maliciously infer any information about the transmitted message.

• The attempt is to realize a transmission in such a way
so as to maximize the transmission rate over the main
channel while keeping the eavesdropper ignorant
about the message.

• Secrecy Capacity:
The rate at which transmitter can use the main link
so as to deliver its message to the legitimate receiver
in a way that the eavesdropper cannot successfully
decode the same information.

\[
C_s = \max_{P_X(x)} \left\{ I(x; y \mid H_B) - I(x; z \mid H_E) \right\}
\]

- Input distribution
- Mutual information over Bob’s channel
- Mutual information over Eve’s channel
A recently proposed transmission scheme for low-complexity implementation of MIMO wireless systems.

- Takes advantage of the location-specific property of the wireless channel.
- Channel coefficients are playing the role of the “modulation unit.”
- Each data block is mapped to a symbol $x_j$ which is then transmitted from the $j$’th antenna.
- With the knowledge of the channel state information (CSI), receiver can detect the activated channel and accordingly detect the transmitted data.
- Spatial modulation (SM) is a more general form of SSK in which a conventional amplitude or phase modulation symbol is spatially modulated (similar to the SSK).
Physical Layer Security for SSK

- To obtain an achievable secrecy rate for SSK as

\[ R_s = \left[ I(x; y \mid H_B) - I(x; z \mid H_E) \right]_{P_X(x)=\frac{1}{M}} \leq C_s \]

\[ I(x; y \mid h_1, h_2, ..., h_M) = \frac{1}{M \pi \sigma_n^2} \sum_{m=1}^{M} \int \exp(-|y - h_m|^2 / \sigma_n^2) \times \log \frac{M \exp(-|y - h_m|^2 / \sigma_n^2)}{\sum_{m'=1}^{M} \exp(-|y - h_{m'}|^2 / \sigma_n^2)} dy \]

\[ y = h_m + n \]

- Precoding

With an assumption that the perfect CSI of the main channel is available at the transmitter, an appropriate precoding can be applied so as to maximize \( d_{ij} \)

- Transmission rate is maximized over the main channel.
- No gain from the eavesdropper’s perspective.
Numerical Results

Legitimate receiver’s SNR is varied while the eavesdropper’s SNR is fixed to 0 dB.

An Example for Precoding

Legitimate receiver’s SNR is varied while the eavesdropper’s SNR is fixed to 0, 12 and 21 dB.

SM is capable of achieving a better secrecy rate with respect to a single-antenna transmission. However, there is a gap between the secrecy rates of SM and a general MIMO system in which all transmit antennas are activated in each time instant.
Conclusion

- Derivation and evaluation of the secrecy capacity is one of the fundamental problems for physical layer security using which we can quantify the maximum rate at which a transmitter can send a message to an intended receiver without being decoded by an eavesdropper.

- An achievable secrecy rate, i.e. a lower bound on the secrecy capacity, was derived and evaluated for SSK which is a recently proposed wireless transmission scheme for low-complexity implementation of MIMO wireless system.

- A precoding scheme which maximizes the minimum Euclidean distance was proposed and the performance improvement achieved by that was evaluated for different number of transmit and receive antennas.

- The framework proposed in this poster can serve as a basis for future studies on SSK in context of secure wireless communications.

References