Improve physical layer security via cooperation

Ning zhang
Outline

• Physical layer security
• Approach based on Multiple antennas
• Cooperation for security
  – Single cooperative relay (with/without jamming)
  – Multiple cooperative relays
• Conclusion
Physical layer security

• **SECURITY** is a critical concern in wireless networks due to the open wireless medium. Any receiver within the range of a wireless transmission can potentially overhear the transmitted information.

• Security against eavesdropping can be achieved by using cryptographic algorithms.
  – However, there are difficulties and vulnerabilities associated with key distribution and management.
  – The implementation of secrecy at higher layers becomes the subject of increasing potential attacks.
  – Sensor or other kind of networks don’t have the seven layers structure and can not support key or …. Without key
  – Physical layer security has its own advantages

• Physical layer security, which exploits the physical characteristics of wireless channels for secure transmission.
Physical layer security
Physical layer security

• Studied for systems with “key-less” security (from a PHY aspect).
• In the above system with a source, destination and eavesdropper.
  – Eavesdropper is “passive”, i.e., eavesdropper does not transmit any signal with the intention of jamming the destination.
  – Eavesdropper only “listens” to the information transmitted by the source.
• The channel between the source and destination is called the “main channel”.
• The channel between the source and eavesdropper is called the “eavesdropper channel”.

Physical layer security

• Is it possible for the source to transmit in such a way that the information can be received properly by the destination but not by the eavesdropper?

• This question is answered by measuring the “secrecy capacity”
Physical layer security

• Secrecy capacity is the difference of the mutual information between the transmitter and the intended receiver versus the eavesdropper.

• Secrecy capacity can be computed the difference between the Shannon capacity of the main channel and that of the eavesdropper channel.
Physical layer security

- Let the Signal-to-Noise ratio (SNR) seen by the destination be $\gamma_{sd}$ and that seen by the eavesdropper be $\gamma_{se}$.
- The Secrecy capacity, $C_s$, for the above system with bandwidth $W$ is given by

$$C_s = \left[ W \log_2 \left( \frac{1+\gamma_{sd}}{1+\gamma_{se}} \right) \right]^+$$

where $x^+ = \max(0, x)$
Physical layer security

\[
C_s = \left[ W \log_2 \left( \frac{1+\gamma_{sd}}{1+\gamma_{se}} \right) \right]^+
\]

• When the eavesdropper channel is a degraded version of the main channel, the source and destination can exchange perfectly secure messages at a nonzero rate, while the eavesdropper can learn almost nothing about the messages from its observations.

• The feasibility of traditional PHY-based security approaches based on single antenna systems is hampered by channel conditions: if the channel between source and destination is worse than the channel between source and eavesdropper, the secrecy capacity is typical zero.
Multiple antennas

- The key idea is that a transmitter can generate noise artificially to conceal the secret message that it is transmitting.
- The noise is generated such that only the eavesdropper is affected but not the intended receiver.
Multiple antennas

- The transmitter transmits $x_k$ at time $k$. The signals received by the legitimate receiver (B) and the eavesdropper (E) are, respectively,
  \[
  z_k = h_k^H x_k + n_k, \\
  y_k = g_k^H x_k + e_k
  \]
  \[
  x_k = p_k u_k + w_k
  \]
  where $u_k$ is the desired signal and $w_k$ is a statistically independent, Gaussian distributed artificial noise.

- Here, **wk is chosen such that** $h_k^H w_k = 0$
  \[
  z_k = h_k^H p_k u_k + n_k, \\
  y_k = g_k^H p_k u_k + g_k^H w_k + e_k
  \]

- Then, the secrecy capacity is given by
  \[
  \log(1 + \frac{|h_k^H p_k|^2 \sigma_u^2}{\sigma_n^2}) - \log(1 + \frac{|g_k^H p_k|^2 \sigma_u^2}{\mathbb{E}[|g_k^H w_k|^2 + \sigma_e^2]})
  \]
One cooperative relay

• Assumptions:
  – Non-direct links: The direct links $S \rightarrow D$ and $S \rightarrow E$ are not available (deep fading) and thus communication is performed via the relay nodes. Eavesdropper cannot overhear the broadcast channel but only the cooperative channel.
  – Clustered applications: The source and there lays are located in the same cluster, while destination and eavesdropper are located outside the cluster.
One cooperative relay

\[ C^{|C_d|}_S(R, J) = \begin{cases} 
0 & \text{if } |C_d| = 0, \\
\left[ \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_{R,D}}{1 + \gamma_{J,D}} \right) \right] & \text{if } |C_d| > 0,
\end{cases} \]

- The selected relay increases the perfect secrecy of the relaying link.
- The selected jammer increases interference at the eavesdropper node to decrease the capacity of eavesdropper link.
One cooperative relay

A. Selection techniques without jamming (a conventional relay)

• 1) Conventional selection (CS):
   This solution does not take into account the eavesdropper channels
   \[ R^* = \arg \max_{R \in C_d} \{ \gamma_{R,D} \}. \]

• 2) Optimal selection (OS):
   This solution takes into account the relay-eavesdroppers links (global instantaneous knowledge for all the links)
   \[ R^* = \arg \max_{R \in C_d} \left\{ \frac{\gamma_{R,D}}{\gamma_{R,E}} \right\} \]

• 3) Suboptimal selection (SS):
   Only average channel knowledge for the eavesdropper link is available
   \[ R^* = \arg \max_{R \in C_d} \left\{ \frac{\gamma_{R,D}}{E[\gamma_{R,E}]} \right\} \]
One cooperative relay

Relay and jammer selection

\[(R^*, J^*) = \arg \max_{\begin{array}{c} R \in C_d, \\
J \in S_{\text{relay}}, \\
R \neq J \end{array}} \left\{ C_S^{(|C_d|)}(R, J) \right\} \]

\[= \arg \max_{\begin{array}{c} R \in C_d, \\
J \in S_{\text{relay}}, \\
R \neq J \end{array}} \left\{ \frac{1}{2} \log_2 \left( \frac{1 + \frac{\gamma_{R, D}}{1 + \gamma_{J, D}}}{1 + \frac{\gamma_{R, E}}{1 + \gamma_{J, E}}} \right) \right\} \]

\[= \arg \max_{\begin{array}{c} R \in C_d, \\
J \in S_{\text{relay}}, \\
R \neq J \end{array}} \left\{ \frac{1 + \frac{\gamma_{R, D}}{1 + \gamma_{J, D}}}{1 + \frac{\gamma_{R, E}}{1 + \gamma_{J, E}}} \right\} \]

\[(R^*, J^*) \approx \arg \max_{\begin{array}{c} R \in C_d, \\
J \in S_{\text{relay}}, \\
R \neq J \end{array}} \left\{ \begin{array}{c} \frac{\gamma_{R, D}}{\gamma_{R, E}} \\
\frac{\gamma_{J, D}}{\gamma_{J, E}} \end{array} \right\} \quad \text{For high SNR cases} \]

\[\Rightarrow \quad \{ \begin{array}{c}
R^* = \arg \max_{R \in C_d} \left\{ \frac{\gamma_{R, D}}{\gamma_{R, E}} \right\} \\
J^* = \arg \min_{J \in \{S_{\text{relay}} - R^*\}} \left\{ \frac{\gamma_{J, D}}{\gamma_{J, E}} \right\} \end{array} \]
Multiple cooperative relays

Two phases and the power of the message signal $s_0$ is normalized to one, i.e, $E\{|s_0|^2\} = 1$.

- $a_i$: baseband complex channel gain between the S and the ith cluster node i,
- $h_i$: channel gain between the ith cluster node and the D,
- $g_{i,j}$: channel gain between the ith cluster node and the jth E.
Multiple cooperative relays

- Phase 1: The source broadcasts its message signal $s0$ locally to its trusted relays within the cluster. The received signal at the $ith$ relay node is $x_i$

$$x_i = \sqrt{P_1}a_is_0 + n_i$$

- Phase 2: Both the source node and all the N−1 trusted relays participate in this stage. For the source node, it transmits a weighted signal of the noiseless signal $s0$, i.e., $w_0s_0$; for the $ith$ relay, it transmits a weighted version of the received noisy signal in Stage 1, i.e., $w_ix_i$, and $w_i$ represents the weight the weight of the $ith$ cluster node.
Multiple cooperative relays

Let us define the vectors $a = [\sqrt{P_1}h_0, \sqrt{P_1}a_1h_1, \ldots, \sqrt{P_1}a_{N-1}h_{N-1}]^\dagger$ and $b_j = [\sqrt{P_1}g_{0,j}, \sqrt{P_1}a_1g_{1,j}, \ldots, \sqrt{P_1}a_{N-1}g_{N-1,j}]^\dagger$ and the $N \times N$ matrices $R_a = aa^\dagger$, $R_b^j = b_j b_j^\dagger$, $U = \text{diag}\{0, |h_1|^2, \ldots, |h_{N-1}|^2\}$, and $V_j = \text{diag}\{0, |g_{1,j}|^2, \ldots, |g_{N-1,j}|^2\}$.

- The received signal at the destination equals

$$y_d = w^\dagger a s_0 + \sum_{i=1}^{N-1} w_i h_i n_i + n_d$$

- Using maximal ratio combining (MRC), the capacity at the destination is

$$C_d = \frac{1}{2} \log_2 \left( \frac{w^\dagger R_a w}{(w^\dagger U w + 1)\sigma^2} \right)$$

where $\alpha \triangleq 1 + P_1|h_0|^2/\sigma^2$
Multiple cooperative relays

• The received signal at the $j$th eavesdropper equals

$$y^j_e = w^\dagger b_j s_0 + \sum_{i=1}^{N-1} w_i g_{i,j} n_i + n^j_e$$

• The capacity at the $j$th eavesdropper is then

$$C^j_e = \frac{1}{2} \log_2 \left( \beta + \frac{w^\dagger R^j_b w}{(w^\dagger V^j w + 1)\sigma^2} \right)$$

where $\beta \triangleq 1 + P_1|g_{0,j}|^2/\sigma^2$.

• The secrecy capacity for $j$th eavesdroppers is defined

$$C_s = \max\{0, C_d - \max(C^1_e, \ldots, C^J_e)\}$$

• Design weights to maximize the secrecy capacity

$$C^j_e = \frac{1}{2} \log_2 \left( \beta + \frac{w^\dagger R^j_b w}{(w^\dagger V^j w + 1)\sigma^2} \right)$$

s.t. $w^\dagger Tw = P_2$ \quad where \quad $T = \text{diag}\{[1, P_1|a_1|^2 + \sigma^2, \ldots, P_1|a_{N-1}|^2 + \sigma^2]\}$
Conclusion

- Physical layer security
- Approaches based on multiple antennas and cooperation are proposed.
- The main objective of these techniques is to boost the capacity of the main channel and decrease the capacity of the eavesdropper channel, simultaneously.
Thanks