Anti-Eavesdropping Channel Estimation (ANECE) for Wireless Security

Yingbo Hua

University of California at Riverside

yhua@ece.ucr.edu

Nov. 27, 2018
GlobalSIP2018 Symposium on SP for WNS

Overview

1. Issues and Approaches
2. Why do we need to make Eve blind to its CSI?
   - Secret-Key-Agreement (SKA) approach
   - Wiretap-Channel (WTC) approach
   - A simple answer
3. How to make Eve blind to its CSI?
   - Prior idea I
   - Prior idea II
   - A new idea: ANECE
4. Conclusion

Issues and Approaches

- Four major issues of wireless security are: authenticity, *confidentiality*, integrity and availability, where *confidentiality against eavesdropping* is a unique challenge and of great interest.
- For confidentiality of large files, using a secret key/password already shared between (legitimate) users is convenient and efficient.
- But no secret key is secure forever, and new secret keys must be generated and distributed to users periodically.
- *Wireless distribution/establishment of secret keys* offers the convenience of mobility and hence is an important problem.
- There are two *complementary* approaches: **secret-key-agreement approach** and **wiretap-channel approach**.

Why to make Eve blind to its CSI - SKA approach

- Assume that Alice obtains $\mathcal{A}$, Bob obtains $\mathcal{B}$, and Eve obtains $\mathcal{E}$. Then, there exists a key agreement protocol, i.e., back-and-forth public communications between Alice and Bob, for both to agree upon a key that is secret from Eve.
- If the joint distribution of $(\mathcal{A}, \mathcal{B}, \mathcal{E})$ is Gaussian with zero mean and known to all parties. Then, the SKA secrecy capacity S_{SKA} in bits per CSI realization satisfies [Bloch and Barros, 2011]:

$$\mathbb{I}(\mathcal{A}, \mathcal{B}) - \min\{\mathbb{I}(\mathcal{A}, \mathcal{E}), \mathbb{I}(\mathcal{B}, \mathcal{E})\} \leq S_{SKA} \leq \min\{\mathbb{I}(\mathcal{A}, \mathcal{B}), \mathbb{I}(\mathcal{A}, \mathcal{B}|\mathcal{E})\}$$

- $\boxed{S_{SKA} = \mathbb{I}(\mathcal{A}, \mathcal{B})}$ if $\mathcal{E}$ is independent of $\mathcal{A}$ and $\mathcal{B}$, which is an ideal situation achievable if
  - $\mathcal{A} = \{\mathcal{A}_T, \mathcal{A}_R\}$ where $\mathcal{A}_T$ and $\mathcal{A}_R$ are respectively transmitted and received by Alice;
  - $\mathcal{B} = \{\mathcal{B}_T, \mathcal{B}_R\}$ where $\mathcal{B}_T$ and $\mathcal{B}_R$ are respectively transmitted and received by Bob; and
  - *Eve is blind to its CSI from both Alice and Bob*.

Why to make Eve blind to its CSI - WTC approach

- Let $\mathbf{H}_{A,B}$ be the channel matrix from Alice (of M_A antennas) to Bob (of M_B antennas), and $\mathbf{H}_{A,E}$ be that from Alice to Eve (of M_E antennas). And the channel noise is white Gaussian of zero mean and unit variance. Then, the WTC secrecy capacity S_{WTC} in bits/s/Hz is [Khisti and Wornell, 2010]

$$S_{WTC} = \max_{tr(\mathbf{Q}_A) \leq P} \left(\log_2 |\mathbf{I}_{M_B} + \mathbf{H}_{A,B}\mathbf{Q}_A\mathbf{H}_{A,B}^H| - \log_2 |\mathbf{I}_{M_E} + \mathbf{H}_{A,E}\mathbf{Q}_A\mathbf{H}_{A,E}^H| \right)$$

  where the CSI anywhere is known everywhere.

- $S_{WTC} = 0$ iff $\lambda_{max}(\mathbf{H}_{A,B}, \mathbf{H}_{A,E}) \doteq \max_{\mathbf{v}} \frac{\|\mathbf{H}_{A,B}\mathbf{v}\|}{\|\mathbf{H}_{A,E}\mathbf{v}\|} \leq 1$, which is generally satisfied when M_E is large enough for any given M_A and M_B.
- $\lim_{P \to \infty} S_{WTC} < \infty$, i.e., S_{WTC} is upper bounded as P increases.
- *What happens if Eve is blind to its CSI?*

Why to make Eve blind to its CSI - WTC approach (Cont.)

- *If Eve is blind to its CSI from Alice* and all entries of $\mathbf{H}_{A,E}$ are i.i.d. with zero mean and variance σ_h^2, then the capacity $C_{A,E}$ of Eve to receive any information from Alice over a time interval of K samples is [Hua, 2018]:

$$C_{A,E} \leq \bar{C}_{A,E} \doteq M_E \log_2(1 + M_A \sigma_h^2 \sigma_x^2) - \frac{M_E}{K} \mathbb{E}\{\log_2 |\mathbf{I}_{M_A} + \sigma_h^2 \mathbf{X}^* \mathbf{X}^T|\}$$

  where σ_x^2 is the variance of each symbol from Alice and $\mathbf{X}$ is the $M_A \times K$ symbol matrix from Alice.
- For $K = M_A$, we can make $\boxed{S_{WTC} = C_{A,B} - C_{A,E} \approx C_{A,B}}$.

  Examples:
  - If $K = M_A = 1$ and all symbols from Alice have a constant amplitude, $\bar{C}_{A,E} = 0$.
  - If $K = M_A \gg 1$, then $\mathbf{X}^* \mathbf{X}^T \approx K \sigma_x^2 \mathbf{I}_{M_A}$ and hence $\bar{C}_{A,E} \approx 0$.
  - For any $K = M_A$, as $P = M_A \sigma_x^2$ increases, $\bar{C}_{A,E}$ is upper bounded by a constant while $C_{A,B}$ scales as $\mathcal{O}(\log_2 P)$.

Why to make Eve blind to its CSI - A simple answer

For both SKA and WTC approaches, if Eve is blind to its CSI,

- a large M_E is no longer a threat, and
- the secrecy capacity does not saturate as P increases.

How to make Eve blind to its CSI - Prior idea I

- Assuming a MISO channel where $\mathbf{h}_{A,B} = \mathbf{h}_{B,A}^T$, [Wang et al, 2015] suggests that if only Bob (of single antenna) sends a training pilot, then Alice can find $\mathbf{h}_{A,B}$ and Eve (of multiple antennas) can find $\mathbf{h}_{B,E}$ (but not $\mathbf{H}_{A,E}$). And then if Alice sends a single-stream signal $x_A(k)$ via beamforming to Bob without any training pilot, then Eve would be unable to detect $x_A(k)$.
- However, *the above idea does not work in practice* because
  - in mobile network, *the actual CSI varies from packet to packet* due to not only changes in the environment but also even the slightest jitters in the high carrier frequency, and
  - hence, in general, the data packet that contains $x_A(k)$ must also contain a training pilot in order for Bob to estimate the (beamformed) effective channel gain $\mathbf{h}_{A,B}^T \hat{\mathbf{h}}_{A,B}^*$ before it can detect $x_A(k)$.

How to make Eve blind to its CSI - Prior idea II

- Another idea was shown in [Chang et al, 2010] where Alice tries to estimate $\mathbf{H}_{A,B}$ via an iterative back-and-forth communications between Alice and Bob. For each transmission from Alice except for the first one, an artificial noise is added to degrade the channel estimation performance at Eve.
- Once again, *the above work overlooked the practical requirement that every packet transmitted must have a training pilot*, or otherwise the intended recipient would most likely fail to receive the desired information.

How to make Eve blind to its CSI - A new idea

- Consider two users (Alice and Bob) with M_A and M_B antennas respectively. Both users are *full-duplex* capable and transmit their packets at the same time as shown here

$\mathbf{P}_A = [\mathbf{p}_A(k_1), k_1 = 1, \cdots, K_1]$	$\mathbf{s}_A(k_2), k_2 = 1, \cdots, K_2$
$\mathbf{P}_B = [\mathbf{p}_B(k_1), k_1 = 1, \cdots, K_1]$	$\mathbf{s}_B(k_2), k_2 = 1, \cdots, K_2$

Table: An example of packets from two users.

- The signal received by Alice for training is $\mathbf{y}_A(k_1) = \mathbf{H}_{B,A}\mathbf{p}_B(k_1) + \mathbf{n}_A(k_1)$ where $\mathbf{n}_A(k_1)$ contains residual self-interference noise whose power is proportional to the power of $\mathbf{p}_A(k_1)$. With a mild condition on $\mathbf{P}_B$, a consistent estimate of $\mathbf{H}_{B,A}$ can be computed at Alice. With $\mathbf{H}_{B,A}$, Alice can decode $\mathbf{s}_B(k_2)$.
- The process at Bob is similar.

How to make Eve blind to its CSI - A new idea (Cont. 1)

- At Eve, the received training signal in $M_E \times K_1$ matrix form is $\mathbf{Y}_E = [\mathbf{G}_A, \mathbf{G}_B] \begin{bmatrix} \mathbf{P}_A \\ \mathbf{P}_B \end{bmatrix} + \mathbf{N}_E$. If $M_B \leq M_A$ and $\mathbf{P}_B$ is chosen to be a subset of $\mathbf{P}_A$, then there is an ambiguity of degree-M_B in $[\mathbf{G}_A, \mathbf{G}_B]$, i.e., $[\mathbf{G}_A, \mathbf{G}_B] \begin{bmatrix} \mathbf{P}_A \\ \mathbf{P}_B \end{bmatrix} = ([\mathbf{G}_A, \mathbf{G}_B] + \mathbf{TN}) \begin{bmatrix} \mathbf{P}_A \\ \mathbf{P}_B \end{bmatrix}$ where $\mathbf{T}$ is an arbitrary $M_E \times M_B$ matrix and $\mathbf{N} \begin{bmatrix} \mathbf{P}_A \\ \mathbf{P}_B \end{bmatrix} = 0$.
- With unknown $[\mathbf{G}_A, \mathbf{G}_B]$, Eve is unable to detect either $\mathbf{s}_A(k_2)$ or $\mathbf{s}_B(k_2)$. Specifically, for $k_2 = 1, \cdots, M_A + M_B$, Eve is totally blind to the information transmitted between Alice and Bob.
- Only if Eve is very close to either Alice or Bob, can it be successful to detect the secret information from Alice or Bob (but not from both).

How to make Eve blind to its CSI - A new idea (Cont. 2)

- Now we consider N full-duplex single-antenna users (such as drones) that concurrently send their packets as follows:

$\mathbf{p}_1^T$	$\mathbf{s}_1^T$	0	0
$\mathbf{p}_2^T$	0	$\mathbf{s}_2^T$	0
$\dots$	$\dots$	$\dots$	$\dots$
$\mathbf{p}_N^T$	0	0	$\mathbf{s}_N^T$

Table: Example of packets from N users.

- The signal received by user i for training can be expressed as $\mathbf{y}_i = \sum_{j \neq i} h_{j,i}\mathbf{p}_j + \mathbf{n}_i$. In order for user i to be able to estimate its CSI $h_{j,i}$ with $j \neq i$ from all other users, we need $\mathbf{P}_i = [\mathbf{p}_j, j \neq i]$ to be of full column rank $N-1$. After the channel estimation, user i can detect $\mathbf{s}_j$ for all $j \neq i$.

How to make Eve blind to its CSI - A new idea (Cont. 3)

- At Eve, the signal received for training is $\mathbf{y}_E = \sum_{j=1}^{N} g_j \mathbf{p}_j + \mathbf{n}_E$. If the (full) pilot matrix $\mathbf{P} = [\mathbf{p}_j, j = 1, \cdots, N]$ also has the rank $N-1$, then Eve is unable to estimate $\mathbf{g}^T \doteq [g_j, j = 1, \cdots, N]$ as there is $\mathbf{c}$ such as $\mathbf{Pg} = \mathbf{P}(\mathbf{g} + \alpha\mathbf{c})$ for any scalar α.
- Without knowing $\mathbf{g}$, Eve is unable to detect the information from all users.
- One good choice of the $K_1 \times N$ matrix $\mathbf{P}$ is such that $K_1 = k_0(N-1)$ and $\mathbf{P}$ has k_0 identical vertical blocks of the $(N-1) \times N$ matrix $\mathbf{Q}$, and $(\mathbf{Q})_{l,i} = \sqrt{P} e^{j2\pi \frac{(l-1)(i-1)}{N}}$ with $l = 1, \cdots, N-1$ and $i = 1, \cdots, N$. Such $\mathbf{P}$ consists of N column vectors equally spaced from each other within a subspace of dimension $N-1$.
- If one or more users are much farther away from Eve than others, then the secret from the closer users are in danger. So, all the users should be relatively clustered together with respect to Eve.

Conclusion

- It is highly beneficial to make Eve (and all Eves) blind to its CSI.
- The prior methods for the above purpose have failed to meet the practical requirement that every packet must have a pilot for channel estimation.
- The new idea called ANECE, which is based on full-duplex radio, appears to be ground-breaking, and should be further studied.

References

- Y. Hua, "Advanced properties of full-duplex radio for securing wireless network", IEEE Trans. SP, pp. 120-135, Jan 1, 2019. (accepted Oct 2018)
- A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas part II: The MIMOME wiretap channel," IEEE Trans. on IT, Nov 2010.
- M. Bloch and J. Barros, Physical-Layer Security, Cambridge Press, 2011.
- T.-H. Chang, et al, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," IEEE Trans. SP, Dec. 2010.
- H.-M. Wang, et al, "Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading," IEEE Trans. WC, Jan. 2015.

Thank You!