Unconditional Secrecy and Computational Complexity against Wireless Eavesdropping

Yingbo Hua and Ahmed Maksud

University of California at Riverside

yhua@ece.ucr.edu, amaks002@ucr.edu

May 2020
Slides for IEEE SPAWC-2020 Online Presentation

Overview

Introduction

- Secrecy unconditional on Eve's channel condition (such as Eve's number of antennas and Eve's noise level) is crucial for many applications.
- Unconditional secrecy (UNS) can be achieved by secret key generation (SKG) utilizing user's reciprocal channel state information (CSI) being independent of Eve's CSI.
- But for (direct) secret information transmission (SIT) between users, there has been little research activity to address UNS.
- In this paper, we evaluate the UNS of several prior methods for SIT and also examine the computational complexities that they impose onto Eve if Eve (with a superior channel condition) wants to break any further secrecy beyond UNS.
- We also show a study of UNS and eavesdropping complexity of a recently proposed method called randomized reciprocal channel modulation (RRCM).

Conventional MIMO Beamforming

- Consider a MIMO channel from Alice to Bob

$$\mathbf{y}_B(k) = \mathbf{H}\mathbf{x}_A(k) + \mathbf{w}_B(k)$$

where $\mathbf{H} \in \mathbb{C}^{N_B \times N_A}$ is the reciprocal channel matrix known to both Alice and Bob (via two-way training) but unknown to Eve.

- Both Alice and Bob know the SVD $\mathbf{H} = \sum_{i=1}^{r} \sigma_i \mathbf{u}_i \mathbf{v}_i^H = \mathbf{U\Sigma V}^H$ with $r = \min(N_A, N_B)$, and Alice transmits

$$\mathbf{x}_A(k) = \mathbf{V}\mathbf{c}_A(k)$$

where $\mathbf{c}_A(k) \in \mathbb{C}^{r\times 1}$ for all k are symbol vectors. We know that Bob can successfully decode all information in $\mathbf{c}_A(k)$ for all k provided that the data rate in the ith element of $\mathbf{c}_A(k)$ is less than the capacity of the ith subchannel.

Conventional MIMO Beamforming (Cont.)

- The signal received by Eve with negligible noise is
$$\mathbf{y}_E(k) = \mathbf{G}_A\mathbf{x}_A(k)$$
where $\mathbf{G}_A \in \mathbb{C}^{N_E \times N_A}$ is known to Eve (due to training pilot from Alice) but unknown to Alice and Bob. Eve with $N_E \geq N_A$ is able to recover $\mathbf{x}_A(k) = \mathbf{V}\mathbf{c}_A(k)$ for all k. But without knowing $\mathbf{V}$, Eve is unable to retrieve all information from $\mathbf{c}_A(k)$.
- However, among all possible random guesses of $\mathbf{c}_A(k)$ for $1 \leq k \leq r$ (for example), there is a correct one. With this correct guess, Eve knows a correct choice of $\mathbf{V}$ by solving the linear equations $\mathbf{x}_A(k) = \mathbf{V}\mathbf{c}_A(k)$ for $1 \leq k \leq r$. Therefore, $\mathbf{x}_A(k)$ for any $k > r$ no longer contains further UNS from Eve.
- In other words, the strict UNS of the above scheme in each coherence period is no more than the entropy of r^2 symbols in $\mathbf{c}_A(k)$ for $1 \leq k \leq r$, and the complexity for Eve to obtain $\mathbf{V}$ mainly involves a set of linear equations, which is in the order of $\mathcal{O}(N_A r^2)$.

Randomized MISO Beamforming

- Li et al introduced a randomized MISO beamforming for a MISO user channel where $N_A > N_B = 1$. The user's channel is described by

$$y_B(k) = \mathbf{h}^T \mathbf{x}_A(k) + \mathbf{w}_B(k)$$

  where $\mathbf{h}$ is known to Alice (through a pilot from Bob) but unknown to Bob, $\mathbf{x}_A(k) = \mathbf{w}_k c_A(k)$ and $\mathbf{w}_k \in \mathbf{C}^{N_A \times 1}$ is randomly chosen for each k subject to

$$\mathbf{h}^T \mathbf{w}_k = \|\mathbf{h}\|.$$

- With $c_A(1)$ (for example) as a training symbol (i.e., known to all), Bob can obtain $\|\mathbf{h}\|$ and hence decode the information in $c_A(k)$ for all $k > 1$ from

$$y_B(k) = \|\mathbf{h}\| c_A(k) + \mathbf{w}_B(k).$$

Randomized MISO Beamforming (Cont.)

- At the same time, Eve with $N_E \geq N_A$ antennas and negligible noise receives
$$\mathbf{y}_E(k) = \mathbf{G}_A \mathbf{x}_A(k) = \mathbf{G}_A \mathbf{w}_k c_A(k)$$
where $\mathbf{G}_A \in \mathbb{C}^{N_E \times N_A}$ is unknown to Eve (or anyone else). With unknown $\mathbf{G}_A \mathbf{w}_k$, Eve is unable to decode all information in $c_A(k)$.
- But if Eve has guessed $c_A(2), \cdots, c_A(N_A)$ correctly (in addition to the known $c_A(1)$), then Eve can compute a vector $\mathbf{q} \in \mathbb{C}^{N_E \times 1}$ such that $\mathbf{q}^H \mathbf{y}_E(k) = c_A(k)$ for $1 \leq k \leq N_A$ or equivalently $\mathbf{q}^H \mathbf{G}_A \mathbf{w}_k = 1$ for $1 \leq k \leq N_A$. Assuming that $\mathbf{w}_1, \cdots, \mathbf{w}_{N_A}$ are linearly independent of each other, $\mathbf{q}^H \mathbf{G}_A$ is unique and hence equals to $\mathbf{h}^T \frac{1}{\|\mathbf{h}\|}$. Then Eve can use the same $\mathbf{q}$ to obtain $\mathbf{q}^H \mathbf{y}_E(k) = c_A(k)$ for all $k > N_A$.
- Therefore, the strict UNS of the above scheme is no more than the entropy of $N_A - 1$ symbols from Alice, and the complexity for Eve to obtain the equalization vector $\mathbf{q}$ is (easy to prove) in the order of $\mathcal{O}(N_E N_A^2)$.

Artificial Noise from Multi-Antenna Transmitter

- Using the artificial noise idea from Negi and Goel, a multi-antenna Alice can transmit

$$\mathbf{x}_A(k) = \mathbf{V}_1\mathbf{s}(k) + \mathbf{V}_2\mathbf{n}(k)$$

  where $\mathbf{s}(k) \in \mathbb{C}^{r_1\times 1}$ with $r_1 \leq r$ is a signal vector, $\mathbf{n}(k) \in \mathbb{C}^{(N_A-r_1)\times 1}$ is an artificial noise meant to jam Eve, $\mathbf{V}_1 = [\mathbf{v}_1, \cdots, \mathbf{v}_{r_1}]$ and $\mathbf{V}_2$ consists of $N_A - r_1$ orthogonal complement vectors of $\mathbf{V}_1$.
- The signal received by Bob is

$$\begin{aligned}\mathbf{y}_B(k) &= \mathbf{H}\mathbf{x}_A(k) + \mathbf{w}_B(k)\\ &= \mathbf{U}_1\mathbf{\Sigma}_1\mathbf{s}(k) + \mathbf{U}_2\mathbf{\Sigma}_2\mathbf{n}(k) + \mathbf{w}_B(k)\end{aligned}$$

  where $\mathbf{U}_1$, $\mathbf{U}_2$, $\mathbf{\Sigma}_1$ and $\mathbf{\Sigma}_2$ are corresponding partitions of $\mathbf{U}$ and $\mathbf{\Sigma}$. Because of $\mathbf{U}_1^H\mathbf{U}_2 = 0$, the artificial noise $\mathbf{n}(k)$ has zero impact on Bob's ability to decode the information from Alice.
- Note that for Bob to estimate $\mathbf{s}(k)$ from $\mathbf{y}_B(k)$, Bob first needs to know $\mathbf{U}_1\mathbf{\Sigma}_1$, which requires (for example) $\mathbf{s}(k)$ for $k = 1, \cdots, r_1$ to be pilot vectors from Alice.

Artificial Noise from Multi-Antenna Transmitter (Cont.)

- Now consider Eve with N_E antennas and negligible (self) noise. Corresponding to $\mathbf{x}_A(k)$ from Alice, the signal received by Eve is

$$\mathbf{y}_E(k) = \mathbf{G}_A\mathbf{V}_1\mathbf{s}(k) + \mathbf{G}_A\mathbf{V}_2\mathbf{n}(k)$$

  where $\mathbf{G}_A$, $\mathbf{V}_1$ and $\mathbf{V}_2$ are all unknowns to Eve.
- But in multipath-rich environment, the entries in $\mathbf{G}_A$ can be modelled to be i.i.d. with zero mean and variance σ_G^2. Then with $N_E \gg 1$ and $N_E \geq N_A$, we have $\frac{1}{N_E}\mathbf{G}_A^H\mathbf{G}_A \approx \sigma_G^2\mathbf{I}_{N_A}$, and hence $\mathbf{G}_A\mathbf{V}_1$ and $\mathbf{G}_A\mathbf{V}_2$ have approximately orthogonal ranges.

Artificial Noise from Multi-Antenna Transmitter (Cont.2)

- Since $\mathbf{s}(1), \cdots, \mathbf{s}(r_1)$ are known pilots, Eve can compute $\mathbf{Q} \in \mathbb{C}^{N_E \times r_1}$ such that
$$\mathbf{Q}^H \mathbf{y}_E(k) \approx \mathbf{s}(k) \quad (1)$$
for $1 \leq k \leq r_1$, or $\sum_{k=1}^{r_1} \|\mathbf{Q}^H \mathbf{y}_E(k) - \mathbf{s}(k)\|^2$ is minimized.
- For large N_E, there exists a $\mathbf{Q} \in \mathit{range}(\mathbf{G}_A \mathbf{V}_1)$ such that $\mathbf{Q}^H \mathbf{G}_A \mathbf{V}_1 \approx \mathbf{I}_{r_1}$ and $\mathbf{Q}^H \mathbf{G}_A \mathbf{V}_2 \approx 0$ and hence (1) holds.
- The solution space of $\mathbf{Q}$ to (1) may be large due to large N_E. But Eve can choose the minimum-norm solution given by $\mathbf{Q}^H = \mathbf{S}(\mathbf{Y}_E^H \mathbf{Y}_E)^{-1} \mathbf{Y}_E$ where $\mathbf{S} = [\mathbf{s}(1), \cdots, \mathbf{s}(r_1)]$ and $\mathbf{Y}_E = [\mathbf{y}_E(1), \cdots, \mathbf{y}_E(r_1)]$.
- Therefore, the strict UNS of the artificial noise scheme is zero, and the complexity for Eve to obtain an accurate equalizer $\mathbf{Q}$ is in order of $\mathcal{O}(r_1^2 N_E)$.

Randomized Reciprocal Channel Modulation (RRCM)

- Consider a MISO user channel with $N_A = n_A^2 \geq 4$ and $N_B = 1$. Using a pilot from Bob, Alice obtains an estimate of $\mathbf{h} = [h_1, \cdots, h_{N_A}]^T$.
- Then, Alice computes $\mathbf{D}_s = diag[m_{s,1}, \cdots, m_{s,N_A}]$ for $1 \leq s \leq S$ as follows. Define $\mathbf{H}_s \in \mathbb{C}^{n_A \times n_A}$ with $(\mathbf{H}_s)_{i,l} = h_{(i-1)n_A+l} m_{s,(i-1)n_A+l}$. Denote the SVD of $\mathbf{H}_s$ as

$$\mathbf{H}_s = \sum_{i=1}^{n_A} \sigma_{i,s} \mathbf{u}_{i,s} \mathbf{v}_{i,s}^H = \mathbf{U}_s \mathbf{\Sigma}_s \mathbf{V}_s^H \quad (2)$$

  where the first element of the vector $\mathbf{u}_{i,s}$ is normalized to be real.
- Also let

$$r_s = \sigma_{1,s} e^{j\mu_{1,s}} \quad (3)$$

  where $\mu_{1,s}$ is the phase of the first element of $\mathbf{v}_{1,s}$. For each s, Alice chooses a sufficiently random r_s to hide the information of c_s in $r_s c_s$, and chooses randomly all other components in $\mathbf{U}_s$, $\mathbf{\Sigma}_s$ and $\mathbf{V}_s$. Then Alice determines $\mathbf{D}_s = diag[m_{s,1}, \cdots, m_{s,N_A}]$ from $\mathbf{H}_s$.

RRCM (Cont.)

- Then, Alice sends a pure and several randomized pilots $\sqrt{P_T}\mathbf{I}_{N_A}, \sqrt{P_T}\mathbf{D}_1\mathbf{I}_{N_A}, \cdots, \sqrt{P_T}\mathbf{D}_S\mathbf{I}_{N_A}$ so that Bob can obtain $\mathbf{h}$ and all entries in $\mathbf{H}_s$. Hence, Bob can use (2) and (3) to compute r_s for $1 \leq s \leq S$.
- Following the randomized pilots, Alice sends $\sqrt{P_T}r_s c_s$ for $1 \leq s \leq S$ from the antenna corresponding to the strongest channel, and then Bob receives

$$y_{B,s} = \sqrt{P_T}h_{max}r_s c_s + w_{B,s}$$

where $h_{max} = arg\max_{h_i}|h_i|$. All channel estimation errors (if not too large) can be lumped into $w_{B,s}$. Since Bob knows $\mathbf{h}$ and r_s, Bob can decode all information in c_s for all s (assuming that the information rate in c_s is so controlled that the probability of detection error is negligible).

RRCM (Cont.2)

- Now consider Eve with $N_E \geq 2$ and negligible noise. Due to the pilots from Alice, Eve knows its receive channel matrix $\mathbf{G}_A$ and also $\mathbf{G}_A\mathbf{D}_s$ for all s. Hence, Eve knows $m_{s,i}$ for all s and i.
- Corresponding to the information symbols from Alice, Eve receives $\mathbf{y}_{E,s} = \mathbf{g}_A r_s c_s$ where $\mathbf{g}_A$ is one of the N_A columns in $\mathbf{G}_A$ and can be identified by Eve. Consequently, Eve knows $r_s c_s$ for all s. In order to decode the information in c_s, Eve must first determine r_s.
- Assume that Eve has guessed correctly c_s for $1 \leq s \leq S_0$ and hence knows r_s for $1 \leq s \leq S_0$. In order to determine r_s for $s > S_0$, Eve now must determine $\mathbf{h}$ using r_s for $1 \leq s \leq S_0$ via (2) along with the conditions $\mathbf{U}_s^H\mathbf{U}_s = \mathbf{I}_{n_A}$ and $\mathbf{V}_s^H\mathbf{V}_s = \mathbf{I}_{n_A}$.
- One can verify that the total number of real unknowns is

  $$N_{unk} = 2n_A^2 + 2(n_A^2 - 1)S_0$$

  and the total number of effective real equations is

  $$N_{equ} = 2n_A^2 S_0.$$

RRCM (Cont.3)

- For a finite number of solutions of $\mathbf{h}$, it is necessary (but not sufficient) that $N_{unk} \leq N_{equ}$ or equivalently $S_0 \geq n_A^2$.
- Hence, the strict amount of UNS of RRCM is no less than the entropy of $N_A = n_A^2$ symbols from Alice.
- Note that (2) is nonlinear. If Eve uses exhaustive search to find $\mathbf{h}$, Eve has to compute the $n_A \times n_A$ SVD for each choice of $\mathbf{h}$. With N_q to be the number of quantization levels for each real element in $\mathbf{h}$, the number of these choices is in the order of $\mathcal{O}(N_q^{2n_A^2})$.
- Alternatively, Eve may apply the Newton's method to search for $\mathbf{h}$ as shown in the paper. The complexity per iteration of the Newton's algorithm is in the order of $\mathcal{O}(N_{unk}^3)$ but there are local extrema due to nonlinearity.

Using the Newton's Method

- For the case of $N_A = 4$, we found that the Newton's method using known r_s for $s = 1, \cdots, S_0$ and $S_0 = 4$ yielded correct solutions of $\mathbf{h}$ from 94% of 100 random initializations of $\mathbf{h}$. We also found that the Newton's method with $S_0 = 5$ yielded a correct solution of $\mathbf{h}$ from each of 100 random initializations.
- For the case of $N_A = 4$, we also considered a phase-only modulation where $r_s = e^{j\mu_{1,s}}$. In this case, using r_s for $s = 1, \cdots, S_0$ and $S_0 \leq 7$, the Newton's method did not find any correct solution of $\mathbf{h}$. With $S_0 = 8$, the Newton's method yielded a correct solution of $\mathbf{h}$ for only 1 out of 500 random initializations. Furthermore, we found that the Newton's method has a very poor convergence property for the phase-only modulation.
- For the case of $N_A = 9$, the necessary condition for a finite number of solutions of $\mathbf{h}$ is now $S_0 \geq 9$. Using $S_0 = 9$, the Newton's method with 1000 random initializations of $\mathbf{h}$ did not converge to any reasonable solution of $\mathbf{h}$. Increasing S_0 did not help either.

Using Exhaustive Search

- We considered the case of $N_A = 9$. To obtain an estimate of how the required computational time varies with N_q (the number of quantization levels of each real element in $\mathbf{h}$), we used our PC with 11.1 Gigaflops to compute the 3×3 SVD (2) for all realizations of $\mathbf{h}$ with $N_q = 2$ and for $s = 1, \cdots, 9$. We recorded this time as T_2.
- Then the required time for N_q is estimated by

$$T_{N_q} = \frac{N_q^{18}}{2^{18}} T_2$$

which is illustrated in the next Figure.

Using Exhaustive Search (Cont.)

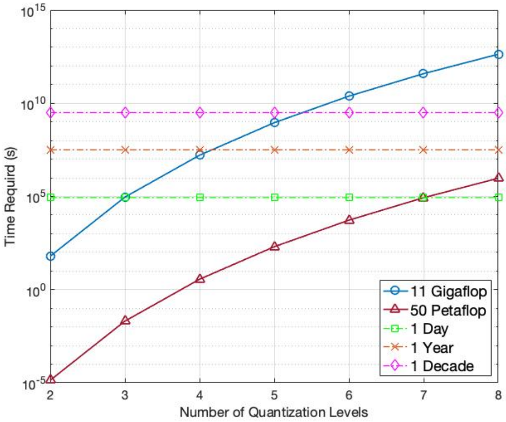

Figure: Computation time required for exhaustive search. Also shown in this figure is the time required if a supercomputer with 50 Petaflops is applied.

Conclusion

Schemes:	MIMO-BF	R-MISO-BF	Artificial-N	RRCM
Symbols with UNS:	r^2 (see below)	$N_A - 1$	0	N_A
Complexity:	$N_A r^2$	$N_E N_A^2$	$N_E r_1^2$	NP

Table: Comparison of UNS and complexities where NP stands for "nondeterministic polynomial", $r \leq \min(N_A, N_B)$, $r_1 \leq \min(r, N_A - 1)$, $N_E \geq N_A$ for R-MISO-BF and Artificial-N, and $N_E \gg 1$ for Artificial-N.

Note that if Alice uses pilot in beamspace for channel training, the UNS of MIMO-BF would be zero.

Thank You!