Unconditional Secrecy and Computational Complexity against Wireless Eavesdropping

Yingbo Hua and Ahmed Maksud
Department of Electrical and Computer Engineering
University of California, Riverside, CA 92521, USA.
Emails: yhua@ece.ucr.edu and ahmed.maksud@email.ucr.edu.

***Abstract*—Unconditional secrecy (UNS) of a wireless transmission scheme refers to the minimum amount of secrecy of the scheme subject to eavesdropping by eavesdropper (Eve) with any number of antennas and any noise level. For each coherence period of wireless channels, the UNS achievable is known to be limited by the entropy of user's reciprocal channel state information (subject to a proper level of quantization). While UNS rate may be too limited for environment with low mobility, it is possible to design physical layer encryption methods to increase the computational complexities that Eve has to overcome in order to break further secrecy beyond UNS. In this paper, we quantify the UNS of several classic transmission schemes and examine the complexity needed to break further secrecy beyond UNS of these schemes. We also provide a UNS and complexity analysis of a recently proposed physical layer encryption scheme called randomized reciprocal channel modulation (RRCM), and show an example where the complexity may exceed Eve's capability.**

***Index Terms*—Network security, end-to-end security, privacy, physical layer security, unconditional secrecy.**

I. Introduction

Communications and data storages via the Internet and Clouds have become indispensable to our lives. Information security is of paramount importance. One of the important security issues is privacy. For the best possible protection of privacy for communications between two parties, they must share their own secret keys. But establishing the shared secret keys initially (without a prior secret key, without physical contact but only through wireless transmissions) is a challenge.

To achieve the above goal, there are many physical layer security methods [1]-[12] which can be grouped under either secret information transmission (SIT) or secrecy key generation (SKG). The SIT schemes include beamforming, artificial noise, cooperative relaying and many varieties of optimizations for maximal secrecy rates of SIT. But unlike SKG schemes, only a limited number of SIT schemes can handle the challenge arising from eavesdropper (Eve) with a large number of antennas, e.g., see [1]-[2]. Many SIT schemes shown in the literature would have zero secrecy if Eve is allowed to have a large number of antennas. We call a secrecy "unconditional secrecy (UNS)" if it is achieved subject to Eve having an unlimited number of antennas and zero noise.

Achieving a positive UNS is possible via either SKG or SIT if the users exploit their own (reciprocal) channel state information (CSI) while Eve's receive CSI is independent of user's CSI. This principle has been widely recognized. But subject to a finite consumption of transmit power (also finite number of antennas on each user and finite number of states of reconfigurable antennas or other cooperative devices for users), the UNS of both SKG and SIT schemes is finite within each coherence period of CSI [13]. For wireless environment with low mobility, the coherence period is long and hence the effective UNS rate in bits/s/Hz can be too limited.

While the strict rate of UNS is limited within each coherence period, a virtual rate of UNS can be significant if Eve fails to overcome a computational complexity at the physical layer created by some physical layer encryption method [14]. One advantage of physical layer encryption (PLE) over network layer encryption (NLE) is that once Eve fails to hack PLE, the secret information is generally not possible to hack later at network layer due to discarded physical layer data. NLE is also known to be vulnerable to quantum computing.

In this paper, we examine the strict amount of UNS of a few prior SIT schemes and also show how easily Eve with a sufficient number of antennas and negligible noise can limit their virtual UNS. (A virtual amount of UNS is the sum of the strict UNS and any further secrecy beyond the strict UNS. The strict UNS is also referred to as UNS.) Furthermore, we examine a new scheme called randomized reciprocal channel modulation (RRCM) [14] and show how much complexity that Eve has to overcome to "limit the virtual UNS of RRCM" or in other words to "break any secrecy beyond UNS".

II. Conventional MIMO Beamforming

Consider a MIMO channel from Alice to Bob

$$\mathbf{y}_B(k) = \mathbf{H}\mathbf{x}_A(k) + \mathbf{w}_B(k) \tag{1}$$

where $\mathbf{H} \in \mathbb{C}^{N_B \times N_A}$ is the reciprocal channel matrix known to both Alice and Bob (via training up to a proper level of quantization) but unknown to Eve. The signal received by Eve with negligible noise is

$$\mathbf{y}_E(k) = \mathbf{G}_A\mathbf{x}_A(k) \tag{2}$$

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. Assume that Alice computes the SVD $\mathbf{H} = \sum_{i=1}^{r} \sigma_i \mathbf{u}_i \mathbf{v}_i^H = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H$ with $r = \min(N_A, N_B)$ and applies $\mathbf{x}_A(k) = \mathbf{V}\mathbf{c}_A(k)$ 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.

978-1-7281-5478-7/20/$31.00 ©2020 IEEE

At the same time, Eve with $N_E \geq N_A$ is able to recover $\mathbf{x}_A(k)$ 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 secret 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 $1 \leq k \leq r$. Also, the computational complexity for Eve to obtain $\mathbf{V}$ mainly involves a linear matrix equation and is in the order of $\mathcal{O}(N_A r^2)$.

III. Randomized MISO Beamforming

In [11], a randomized MISO beamforming is introduced for a MISO user channel where $N_A > N_B = 1$. Namely, the user's channel can be described by

$$y_B(k) = \mathbf{h}^T \mathbf{x}_A(k) + \mathbf{w}_B(k) \tag{3}$$

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

At the same time, Eve with $N_E \geq N_A$ antennas and negligible noise receives

$$\mathbf{y}_E(k) = \mathbf{G}_A \mathbf{x}_A(k) = \mathbf{G}_A \mathbf{w}_k c_A(k) \tag{4}$$

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 scheme in [11] is no more than the entropy of $N_A - 1$ symbols from Alice, and the computational complexity for Eve to obtain the equalization vector $\mathbf{q}$ is (easy to prove) in the order of $\mathcal{O}(N_E N_A^2)$.

IV. Artificial Noise from Multi-Antenna Transmitter

An artificial noise scheme was introduced in [12] where the transmitted signal vector from a multi-antenna Alice has the following form $\mathbf{x}_A(k) = \mathbf{V}_1 \mathbf{s}(k) + \mathbf{V}_2 \mathbf{n}(k)$ 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

$$\begin{aligned} \mathbf{y}_B(k) &= \mathbf{H}\mathbf{x}_A(k) + \mathbf{w}_B(k) \\ &= \mathbf{U}_1 \mathbf{\Sigma}_1 \mathbf{s}(k) + \mathbf{U}_2 \mathbf{\Sigma}_2 \mathbf{n}(k) + \mathbf{w}_B(k) \end{aligned} \tag{5}$$

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 Alice knows the user's MIMO channel matrix $\mathbf{H}$ due to a previous pilot from Bob. But for Bob to estimate $\mathbf{s}(k)$ from $\mathbf{y}_B(k)$, Bob first needs to know $\mathbf{U}_1 \mathbf{\Sigma}_1$, which can be achieved by choosing $\mathbf{s}(k)$ for $k = 1, \cdots, r_1$ to be pilot vectors from Alice.

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

$$\mathbf{y}_E(k) = \mathbf{G}_A \mathbf{V}_1 \mathbf{s}(k) + \mathbf{G}_A \mathbf{V}_2 \mathbf{n}(k) \tag{6}$$

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.

Since $\mathbf{s}(1), \cdots, \mathbf{s}(r_1)$ are pilot vectors from Alice, Eve can compute $\mathbf{Q} \in \mathbb{C}^{N_E \times r_1}$ such that

$$\mathbf{Q}^H \mathbf{y}_E(k) \approx \mathbf{s}(k) \tag{7}$$

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 $\mathbf{Q} \in range(\mathbf{G}_A \mathbf{V}_1)$ 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 (7) holds. The solution space of $\mathbf{Q}$ to (7) is large due to large N_E. The minimum norm solution is 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 $\mathcal{O}(r_1^2 N_E)$.

V. Randomized Reciprocal Channel Modulation (RRCM)[14]

Consider the case of $N_A = n_A^2 \geq 4$ and $N_B = 1$ (although the RRCM principle as shown below is applicable for any $N_A \geq 1$ and $N_B \geq 1$). Using a pilot from Bob, Alice obtains the channel vector $\mathbf{h} = [h_1, \cdots, h_{N_A}]^T$.

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

$$\mathbf{H}_s = \sum_{i=1}^{n_A} \sigma_{i,s} \mathbf{u}_{i,s} \mathbf{v}_{i,s}^H = \mathbf{U}_s \mathbf{\Sigma}_s \mathbf{V}_s^H \tag{8}$$

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

$$r_s = \sigma_{1,s} e^{j\mu_{1,s}} \tag{9}$$

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 also chooses randomly all other components in $\mathbf{U}_s$, $\mathbf{\Sigma}_s$ and $\mathbf{V}_s$ (subject to some bound constraint on each diagonal entry of $\mathbf{\Sigma}_s$ for reliable reception at Bob). Then Alice determines $\mathbf{D}_s = diag[m_{s,1}, \cdots, m_{s,N_A}]$ from $\mathbf{H}_s$.

(Any realization of $\mathbf{D}_s$ could be rejected if any of its diagonal entries is too small.)

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 (8) and (9) to compute r_s for $1 \le s \le S$.

Following the randomized pilots, Alice also sends $\sqrt{P_T}r_s c_s$ for $1 \le s \le S$ 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).

Now consider Eve with $N_E \ge 2$ 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 $1 \le s \le S_0$ and hence knows r_s for $1 \le s \le S_0$. In order to determine r_s for $s > S_0$, Eve now must determine $\mathbf{h}$ using r_s for $1 \le s \le S_0$ via (8) 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 (i.e., those in $\mathbf{h}$ and all other unknowns in the SVD equation (8)) is $N_{unk} = 2n_A^2 + 2(n_A^2 - 1)S_0$ and the total number of effective real equations is $N_{equ} = 2n_A^2 S_0$. For a finite number of solutions of $\mathbf{h}$, it is necessary (but not sufficient) that $N_{unk} \le N_{equ}$ or equivalently $S_0 \ge n_A^2$.

Hence, the strict amount of UNS of RRCM is no less than the entropy of n_A^2 symbols from Alice. Note that (8) 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 Appendix VII-A. The complexity per iteration of the Newton's algorithm is in the order of $\mathcal{O}(N_{unk}^3)$.

Unlike the previous schemes, RRCM forces Eve to solve a nonlinear inverse problem to obtain user's CSI. Further insight is shown next.

VI. Simulation of Eve's Complexity to Break RRCM

A. Using the Newton's Method

1) Four Channel Unknowns: Consider $N_A = 4$ and $N_B = 1$. It follows that

$$\mathbf{H}_s = \begin{bmatrix} h_1 m_{s,1} & h_2 m_{s,2} \\ h_3 m_{s,3} & h_4 m_{s,4} \end{bmatrix} \tag{10}$$

where each element of $\mathbf{h} = [h_1, \cdots, h_4]^T$ was randomly chosen from $\mathcal{CN}(0,1)$, and $\mathbf{m}_s = [m_{s,1}, \cdots, m_{s,4}]$ for each s was so chosen that r_s defined via (8) and (9) is sufficiently random (and the singular values have sufficient distances from each other). Assume that Eve has correctly guessed c_s for $s = 1, \cdots, S_0$ and hence Eve now knows r_s for $s = 1, \cdots, S_0$. We simulated the Newton's method to find $\mathbf{h}$ using r_s for $s = 1, \cdots, S_0$. For $S_0 = 4$, the Newton's method yielded correct solutions of $\mathbf{h}$ from 94% of 100 random initializations of $\mathbf{h}$. (Note that the correct solutions of $\mathbf{h}$ include those that may be different from $\mathbf{h}$ but yield the same r_s via the SVD (8) for all s including $s > S_0$.) But for $S_0 = 5$, the Newton's method yielded a correct solution of $\mathbf{h}$ from each of 100 random initializations.

We also tested a phase-only modulation where $r_s = e^{j\mu_{1,s}}$. In this case, the number of unknowns is no larger than the number of equations if and only if $S_0 \ge 8$. It is somewhat expected that using r_s for $s = 1, \cdots, S_0$ with $S_0 \le 7$, the Newton's method did not find any correct solution of $\mathbf{h}$. But for $S_0 = 8$, the Newton's method yielded a correct solution of $\mathbf{h}$ (valid for all s) from 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.

2) Nine Channel Unknowns: Consider $N_A = 9$ and $N_B = 1$. In this case, $\mathbf{H}_s$ is 3×3 and $\mathbf{h}$ is 9×1. The necessary condition on S_0 for a finite number of solutions of $\mathbf{h}$ is now $S_0 \ge 9$. But with $S_0 = 9$, the Newton's method with 1000 random initializations of $\mathbf{h}$ did not even converge to a reasonable solution of $\mathbf{h}$ that is valid for $1 \le s \le S_0$. In other words, the Newton's method could not handle this case in our simulation.

This is apparently due to the nonlinearity of the problem. And an effective degree of nonlinearity for each unknown in (8) increases as the dimension of $\mathbf{h}$ increases. (For a set of n arbitrary second-order polynomial equations with n unknowns, for example, the number of possible solutions from these equations could be up to 2^n.)

B. Using Exhaustive Search

Since the Newton's method could not handle the case with 9 channel unknowns, we now consider the exhaustive search over a discrete space $\mathcal{S}_\mathbf{h}$ of the 9×1 complex vector $\mathbf{h}$. For each $\mathbf{h} \in \mathcal{S}_\mathbf{h}$, we need to compute the SVD (8) for $s = 1, \cdots, S_0$ with $S_0 = 9$. (A correct solution of $\mathbf{h}$ might be found with a nonzero probability if the consequent r_s for $s = 1, \cdots, S_0$ from (9) match the "known" r_s for $s = 1, \cdots, S_0$.) With N_q quantization levels for each real component in $\mathbf{h}$, we have $|\mathcal{S}_\mathbf{h}| = N_q^{18}$. To obtain an estimate of how the required computational time varies with N_q, we used our PC with 11.1 Gigaflops to compute the 3×3 SVD (8) 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 can be estimated by $T_{N_q} = \frac{N_q^{18}}{2^{18}}T_2$, which is illustrated in Fig. 1. Also shown in this figure is the time required if a supercomputer with 50 Petaflops is applied here. For easy reference, we have also marked the times for 1 day, 1 year and 1 decade.

We see that with just $N_q = 8$ (or 3 bits for each real component of $\mathbf{h}$), finding $\mathbf{h}$ using the exhaustive search could

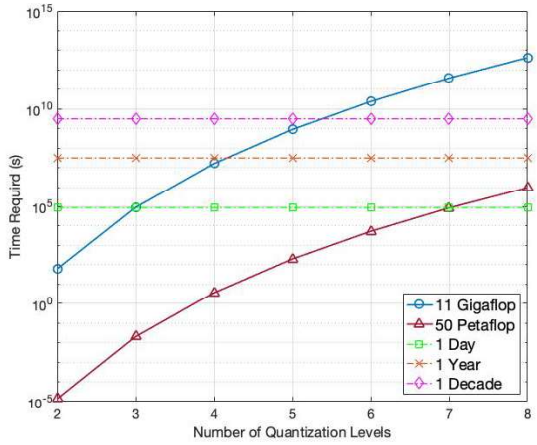

Fig. 1. Computation Time Required for exhaustive Search

require more than a decade on our PC or more than a day on a supercomputer. With a randomized exhaustive search, the averaged time required to find a correct solution of $\mathbf{h}$ can be reduced by a factor, but the order of complexity $\mathcal{O}(N_q^{2N_A})$ as discussed before does not change.

Subject to Eve's failure to obtain a correct solution of $\mathbf{h}$ (and hence r_s for any $s \geq S_0$) based on random guesses of c_s for $s = 1, \cdots, S_0$, all information in c_s for all s transmitted from Alice to Bob remains secure from Eve with any number of antennas and any noise level.

VII. Conclusion

In this paper, we have examined the unconditional secrecy (UNS) of several classic information transmission schemes subject to eavesdropping by Eve with unlimited number of antennas and/or negligible noise. We showed that the conventional MIMO beamforming method for Alice with N_A antennas and Bob with N_B antennas can provide an UNS no more than the entropy of r symbol vectors from Alice where $r = \min(N_A, N_B)$, a randomized MISO beamformer for $N_A > N_B = 1$ can provide an UNS no more than the entropy of $N_A - 1$ symbols from Alice, and the artificial noise scheme for any N_A and N_B can provide only zero UNS. And the complexity for Eve to break the secrecy beyond the UNS for any of the above schemes is shown to be highly feasible. We also examined a new scheme called randomized reciprocal channel modulation (RRCM) proposed in [14]. For a MISO user channel with $N_A \geq N_B = 1$, the UNS of RRCM can be up to the entropy of N_A transmitted symbols from Alice. Furthermore, we found via simulation that for $N_A \geq 9$ the computational complexity for Eve to break the secrecy beyond the UNS of RRCM is infeasible on a PC with 11 Gigaflops or even on a supercomputer depending on the delay requirement. The potential applications of RRCM as physical layer encryption include satellite communications where network layer encryption is increasingly threatened by quantum computing (due to Shor's algorithm).

Appendix

A. The Newton's method applicable by Eve

Let $\mathbf{H}_s \in \mathbb{C}^{M\times N}$ be such that $(\mathbf{H}_s)_{i,j} = m_{s,i,j}h_{i,j}$ with $M \leq N$. The SVD of $\mathbf{H}_s$ is denoted by

$$\mathbf{H}_s = \mathbf{U}_s\mathbf{\Sigma}_s\mathbf{V}_s^H \tag{11}$$

with $\mathbf{U}_s \in \mathbb{C}^{M\times M}$, $\mathbf{V}_s \in \mathbb{C}^{N\times M}$ and $\mathbf{\Sigma}_s \in \mathbb{R}^{M\times M}$. Also $\mathbf{V}_s^H\mathbf{V}_s = \mathbf{I}_M$ and $\mathbf{U}_s^H\mathbf{U}_s = \mathbf{I}_M$. The number of real equations in the SVD for $s = 1, \cdots, S$ is $N_{equ} = 2MNS + 2M^2S$, and the number of real unknowns in the SVD is $N_{unk} = 2MNS + 2M^2S$ where the first row of either $\mathbf{U}_s$ or $\mathbf{V}_s$ has zero phases.

Let $r_s = \sigma_s e^{j\mu_s}$ where σ_s is a singular value of $\mathbf{H}_s$ and μ_s is a phase of one of the elements in $\mathbf{U}_s$ or $\mathbf{V}_s$.

We can write $\mathbf{H}_s = \mathbf{M}_s \odot \mathbf{H}$. If $\mathbf{H}$ consists of $K \leq MN$ complex unknowns and r_s for $s = 1, \cdots, S$ is known, then we need $S \geq K$ in order to determine $\mathbf{H}$ from r_s for $s = 1, \cdots, S$.

By partial differentiation, we have

$$\mathbf{M}_s \odot \partial\mathbf{H} = \partial\mathbf{U}_s\mathbf{\Sigma}_s\mathbf{V}_s^H + \mathbf{U}_s\partial\mathbf{\Sigma}_s\mathbf{V}_s^H + \mathbf{U}_s\mathbf{\Sigma}_s\partial\mathbf{V}_s^H \tag{12}$$

We know that $vec(\mathbf{M}_s \odot \partial\mathbf{H}) = vec(\mathbf{M}_s) \odot vec(\partial\mathbf{H}) = \mathbf{m}_s \odot \partial\mathbf{h} = \mathbf{D}_{m,s}\partial\mathbf{h}$ where $\mathbf{D}_{m,s} = diag(\mathbf{m}_s)$; $vec(\partial\mathbf{U}_s\mathbf{\Sigma}_s\mathbf{V}_s^H) = (\mathbf{V}_s^*\mathbf{\Sigma}_s \otimes \mathbf{I}_M)\partial\mathbf{u}_s$; $vec(\mathbf{U}_s\partial\mathbf{\Sigma}_s\mathbf{V}_s^H) = (\mathbf{V}_s^* \otimes \mathbf{I}_M)vec(\mathbf{U}_s\partial\mathbf{\Sigma}_s) = (\mathbf{V}_s^* \otimes \mathbf{I}_M)\mathbf{D}_{U,s}\partial\boldsymbol{\sigma}_s$ where $\mathbf{D}_{U,s} = diag((\mathbf{U}_s)_1, \cdots, (\mathbf{U}_s)_M)$; and $vec(\mathbf{U}_s\mathbf{\Sigma}_s\partial\mathbf{V}_s^H) = (\mathbf{I}_N \otimes \mathbf{U}_s\mathbf{\Sigma}_s)\mathbf{P}_v\partial\mathbf{v}_s^*$ where $\mathbf{P}_v\mathbf{v}_s = vec(\mathbf{V}_s^T)$. Therefore, (12) is equivalent to

$$\begin{aligned}\mathbf{D}_{m,s}\partial\mathbf{h} =& (\mathbf{V}_s^*\mathbf{\Sigma}_s \otimes \mathbf{I}_M)\partial\mathbf{u}_s + (\mathbf{V}_s^* \otimes \mathbf{I}_M)\mathbf{D}_{U,s}\partial\boldsymbol{\sigma}_s \\ &+ (\mathbf{I}_N \otimes \mathbf{U}_s\mathbf{\Sigma}_s)\mathbf{P}_v\partial\mathbf{v}_s^*.\end{aligned} \tag{13}$$

Also by partial differentiation, we have $\partial\mathbf{V}_s^H\mathbf{V}_s + \mathbf{V}_s^H\partial\mathbf{V}_s = 0$ which is equivalent to

$$(\mathbf{V}_s^T \otimes \mathbf{I}_M)\mathbf{P}_v\partial\mathbf{v}_s^* + (\mathbf{I}_M \otimes \mathbf{V}_s^H)\partial\mathbf{v}_s = 0. \tag{14}$$

Similarly, we have

$$(\mathbf{U}_s^T \otimes \mathbf{I}_M)\mathbf{P}_u\partial\mathbf{u}_s^* + (\mathbf{I}_M \otimes \mathbf{U}_s^H)\partial\mathbf{u}_s = 0. \tag{15}$$

where $\mathbf{P}_u\mathbf{u}_s = vec(\mathbf{U}_s^T)$.

Let $\mathbf{x} = [\mathbf{x}_1^T, \mathbf{x}_2^T, \mathbf{x}_3^T, \mathbf{x}_4^T]^T$ where $\mathbf{x}_1 = [\Re(\mathbf{h})^T, \Im(\mathbf{h})^T]^T$, $\mathbf{x}_2 = [\Re(\mathbf{u}_1)^T, \Im(\mathbf{u}_1)^T, \cdots, \Re(\mathbf{u}_S)^T, \Im(\mathbf{u}_S)^T]^T$, $\mathbf{x}_3 = [\Re(\mathbf{v}_1)^T, \Im(\mathbf{v}_1)^T, \cdots, \Re(\mathbf{v}_S)^T, \Im(\mathbf{v}_S)^T]^T$, and $\mathbf{x}_4 = [\boldsymbol{\sigma}_1^T, \cdots, \boldsymbol{\sigma}_S^T]^T$. The above differential equations are equivalent to

$$\mathbf{Y}\partial\mathbf{x} = 0 \tag{16}$$

where

$$\mathbf{Y} = \begin{bmatrix} \mathbf{Y}_{1,1} & \mathbf{Y}_{1,2} & \mathbf{Y}_{1,3} & \mathbf{Y}_{1,4} \\ 0 & \mathbf{Y}_{2,2} & 0 & 0 \\ 0 & 0 & \mathbf{Y}_{3,3} & 0 \end{bmatrix} \tag{17}$$

$$\mathbf{Y}_{1,1} = \begin{bmatrix} -\Re(\mathbf{D}_{m,1}) & \Im(\mathbf{D}_{m,1}) \\ -\Im(\mathbf{D}_{m,1}) & -\Re(\mathbf{D}_{m,1}) \\ \cdots & \cdots \\ -\Re(\mathbf{D}_{m,S}) & \Im(\mathbf{D}_{m,S}) \\ -\Im(\mathbf{D}_{m,S}) & -\Re(\mathbf{D}_{m,S}) \end{bmatrix} \tag{18}$$

$$\mathbf{Y}_{1,2} = diag(\mathbf{Y}_{1,2,1}, \cdots, \mathbf{Y}_{1,2,S}) \tag{19}$$

$$\mathbf{Y}_{1,2,s} = \begin{bmatrix} \Re(\mathbf{V}_s^* \mathbf{\Sigma}_s \otimes \mathbf{I}_M) & -\Im(\mathbf{V}_s^* \mathbf{\Sigma}_s \otimes \mathbf{I}_M) \\ \Im(\mathbf{V}_s^* \mathbf{\Sigma}_s \otimes \mathbf{I}_M) & \Re(\mathbf{V}_s^* \mathbf{\Sigma}_s \otimes \mathbf{I}_M) \end{bmatrix} \tag{20}$$

$$\mathbf{Y}_{1,3} = diag(\mathbf{Y}_{1,3,1}, \cdots, \mathbf{Y}_{1,3,S}) \tag{21}$$

$$\mathbf{Y}_{1,3,s} = \begin{bmatrix} \Re((\mathbf{I}_N \otimes \mathbf{U}_s \mathbf{\Sigma}_s)\mathbf{P}_v) & \Im((\mathbf{I}_N \otimes \mathbf{U}_s \mathbf{\Sigma}_s)\mathbf{P}_v) \\ \Im((\mathbf{I}_N \otimes \mathbf{U}_s \mathbf{\Sigma}_s)\mathbf{P}_v) & -\Re((\mathbf{I}_N \otimes \mathbf{U}_s \mathbf{\Sigma}_s)\mathbf{P}_v) \end{bmatrix} \tag{22}$$

$$\mathbf{Y}_{1,4} = diag(\mathbf{Y}_{1,4,1}, \cdots, \mathbf{Y}_{1,4,S}) \tag{23}$$

$$\mathbf{Y}_{1,4,s} = \begin{bmatrix} \Re((\mathbf{V}_s^* \otimes \mathbf{I}_M)\mathbf{D}_{U,s}) \\ \Im((\mathbf{V}_s^* \otimes \mathbf{I}_M)\mathbf{D}_{U,s}) \end{bmatrix} \tag{24}$$

$$\mathbf{Y}_{2,2} = diag(\mathbf{Y}_{2,2,1}, \cdots, \mathbf{Y}_{2,2,S}) \tag{25}$$

$$\mathbf{Y}_{2,2,s} = \begin{bmatrix} \Re((\mathbf{U}_s^T \otimes \mathbf{I}_M)\mathbf{P}_u + (\mathbf{I}_M \otimes \mathbf{U}_s^H)), \\ \Im((\mathbf{U}_s^T \otimes \mathbf{I}_M)\mathbf{P}_u + (\mathbf{I}_M \otimes \mathbf{U}_s^H)), \\ \Im((\mathbf{U}_s^T \otimes \mathbf{I}_M)\mathbf{P}_u - (\mathbf{I}_M \otimes \mathbf{U}_s^H)) \\ \Re(-(\mathbf{U}_s^T \otimes \mathbf{I}_M)\mathbf{P}_u + (\mathbf{I}_M \otimes \mathbf{U}_s^H)) \end{bmatrix} \tag{26}$$

$$\mathbf{Y}_{3,3} = diag(\mathbf{Y}_{3,3,1}, \cdots, \mathbf{Y}_{3,3,S}) \tag{27}$$

$$\mathbf{Y}_{3,3,s} = \begin{bmatrix} \Re((\mathbf{V}_s^T \otimes \mathbf{I}_M)\mathbf{P}_v + (\mathbf{I}_M \otimes \mathbf{V}_s^H)), \\ \Im((\mathbf{V}_s^T \otimes \mathbf{I}_M)\mathbf{P}_v + (\mathbf{I}_M \otimes \mathbf{V}_s^H)), \\ \Im((\mathbf{V}_s^T \otimes \mathbf{I}_M)\mathbf{P}_v - (\mathbf{I}_M \otimes \mathbf{V}_s^H)) \\ \Re(-(\mathbf{V}_s^T \otimes \mathbf{I}_M)\mathbf{P}_v + (\mathbf{I}_M \otimes \mathbf{V}_s^H)) \end{bmatrix}. \tag{28}$$

It is important to note that for each and every known element in $\mathbf{x}$, we should remove the corresponding elements in $\partial\mathbf{x}$ and also remove the corresponding columns in $\mathbf{Y}$.

Then the linear approximation for the SVD equations around $\mathbf{x} = \mathbf{x}_n$ is

$$\mathbf{f}(\mathbf{x}) \approx \mathbf{f}(\mathbf{x}_n) + \mathbf{Y}(\mathbf{x} - \mathbf{x}_n) \tag{29}$$

where

$$\mathbf{f}^T(\mathbf{x}) = \left[\mathbf{f}_1^T(\mathbf{x}), \mathbf{f}_2^T(\mathbf{x}), \mathbf{f}_3^T(\mathbf{x})\right] \tag{30}$$

$$\mathbf{f}_1^T(\mathbf{x}) = [\mathbf{f}_{1,1}^T(\mathbf{x}), \cdots, \mathbf{f}_{1,S}^T(\mathbf{x})] \tag{31}$$

$$\mathbf{f}_{1,s}(\mathbf{x}) = \begin{bmatrix} \Re(vec(-\mathbf{H}_s + \mathbf{U}_s \mathbf{\Sigma}_s \mathbf{V}_s^H)) \\ \Im(vec(-\mathbf{H}_s + \mathbf{U}_s \mathbf{\Sigma}_s \mathbf{V}_s^H)) \end{bmatrix} \tag{32}$$

$$\mathbf{f}_2^T(\mathbf{x}) = [\mathbf{f}_{2,1}^T(\mathbf{x}), \cdots, \mathbf{f}_{2,S}^T(\mathbf{x})] \tag{33}$$

$$\mathbf{f}_{2,s}(\mathbf{x}) = \begin{bmatrix} \Re(vec(\mathbf{U}_s^H \mathbf{U}_s - \mathbf{I}_M)) \\ \Im(vec(\mathbf{U}_s^H \mathbf{U}_s - \mathbf{I}_M)) \end{bmatrix} \tag{34}$$

$$\mathbf{f}_3^T(\mathbf{x}) = [\mathbf{f}_{3,1}^T(\mathbf{x}), \cdots, \mathbf{f}_{3,S}^T(\mathbf{x})] \tag{35}$$

$$\mathbf{f}_{3,s}(\mathbf{x}) = \begin{bmatrix} \Re(vec(\mathbf{V}_s^H \mathbf{V}_s - \mathbf{I}_M)) \\ \Im(vec(\mathbf{V}_s^H \mathbf{V}_s - \mathbf{I}_M)) \end{bmatrix} \tag{36}$$

The Newton's algorithm to search for $\mathbf{x}_{opt}$ such that $\mathbf{f}(\mathbf{x}_{opt}) = 0$ is

$$\mathbf{x}_{n+1} = \mathbf{x}_n - (\mathbf{Y}^T\mathbf{Y})^{-1}\mathbf{Y}^T\mathbf{f}(\mathbf{x}_n) \tag{37}$$

Note that $\mathbf{x}$ has $N_x = 2(MNS + M^2S + K - S)$ real elements, and $\mathbf{f}(\mathbf{x})$ has $N_f = 2(MNS + 2M^2S)$ real entries but with $2M^2S$ redundant entries. The redundance comes from the symmetry of $\mathbf{U}_s^H\mathbf{U}_s = \mathbf{I}_M$ and $\mathbf{V}_s^H\mathbf{V}_s = \mathbf{I}_M$. Removing the redundant entries can save computational time.

To remove the redundance, we should remove the elements in $\mathbf{f}_{2,s}(\mathbf{x})$ corresponding to those below the diagonal of $\Re(\mathbf{U}_s^H\mathbf{U}_s - \mathbf{I}_M)$ and those on and below the diagonal of $\Im(\mathbf{U}_s^H\mathbf{U}_s - \mathbf{I}_M)$, and we should also remove the elements in $\mathbf{f}_{3,s}(\mathbf{x})$ corresponding to those below the diagonal of $\Re(\mathbf{V}_s^H\mathbf{V}_s - \mathbf{I}_M)$ and those on and below the diagonal of $\Im(\mathbf{V}_s^H\mathbf{V}_s - \mathbf{I}_M)$. Consequently, we must also remove the corresponding rows in $\mathbf{Y}$ in the Newton's algorithm.

Also note that after each iteration for $\mathbf{x}$, an estimate of $\mathbf{h}$ should be retrieved from a corresponding part of $\mathbf{x}$ and be used via (8) to reset the other part of $\mathbf{x}$. This operation substantially improves the convergence property of the Newton's algorithm.

For each iteration, the computational complexity of the Newton's algorithm is dominated by the $N_x \times N_x$ inverse $(\mathbf{Y}^T\mathbf{Y})^{-1}$ which has the complexity order $\mathcal{O}(N_x^3)$.

ACKNOWLEDGMENT

This work was supported in part by the Army Research Office under Grant Number W911NF-17-1-0581.

REFERENCES

[1] R. Sohrabi, Q. Zhu, and Y. Hua, "Secrecy analyses of a full-duplex MIMOME network," IEEE Transactions on Signal Processing, Vol. 67, No. 23, pp. 5968-5982, Dec. 2019.

[2] Y. Hua, "Advanced properties of full-duplex radio for securing wireless network," IEEE Transactions on Signal Processing, Vol. 67, No. 1, pp. 120-135, Jan. 2019.

[3] C. Song, "Leakage rate analysis for artificial noise assisted massive MIMO with non-coherent passive eavesdropper in block-fading," IEEE Transactions on Wireless Communications, Vol. 18, No. 4, pp. 2111-2124, April 2019.

[4] H. V. Poor and R. F. Schaefer, "Wireless physical layer security", PNAS, Vol. 114, no. 1, pp.19-26, January 3, 2017.

[5] M. Bloch and J. Barros, Physical-Layer Security, Cambridge Press, 2011.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," IEEE Journal on Selected Areas in Communications, Vol. 36, No. 4, April 2018.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas part II: The MIMOME wiretap channel," IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515-5532, Nov 2010.

[8] H. Hentila, V. Koivunen, H. V. Poor, R. S. Blum, "Secure key generation for distributed inference in IoT", 53rd Annual Conference on Information Sciences and Systems (CISS), 2019.

[9] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading," IEEE Trans. Wireless Communications, Vol. 14, No. 1, pp. 94-106, Jan. 2015.

[10] T.-H. Chang, W.-C. Chiang, Y.-W. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," IEEE Trans. Signal Processing, Vol. 58, No. 12, pp. 6223-6237, Dec. 2010.

[11] X. Li, J Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions", Journal of Communications, Vol. 2, No. 3, May 2007.

[12] R. Negi and S. Goel, "Secret communication using artificial noise", IEEE 62nd Vehicular Technology Conference, Vol. 3, pp. 1906-1910, Sept 2005.

[13] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," IEEE Transactions on Information Theory, Vol. 58, No. 5, pp. 2838-2849, May 2012.

[14] Y. Hua, "Reliable and secure transmissions for future networks," IEEE ICASSP'2020, pp.2560-2564, May 2020.