RELIABLE AND SECURE TRANSMISSION FOR FUTURE NETWORKS

Yingbo Hua
Department of Electrical and Computer Engineering
University of California, Riverside, CA 92521, USA. Email: yhua@ece.ucr.edu.

***Abstract*—This paper introduces a novel physical layer encryption method called randomized reciprocal channel modulation (RRCM) for reliable and secure transmission of information against eavesdropper (Eve) with any number of antennas and any noise level. RRCM makes it computationally complex for Eve to estimate the user's channel state information (CSI) that is used to scramble the information symbols transmitted between users. Subject to Eve's failure to overcome the physical-layer computational complexity, users can apply RRCM to achieve a virtually constant (significant) rate in bits/s/Hz of unconditional secrecy - unconditional on Eve's number of antennas, Eve's noise level and the CSI coherence time.**

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

I. INTRODUCTION

Future wireless networks promise to provide ultra fast connections for people-to-people, devices-to-devices, devices-to-people and people-to-devices communications around the world. Yet, questions on security issues are abundant, which hinders the development of ultra fast networks for the benefit of humanity.

One important security question of interest in this paper is privacy. Like current networks, future networks will continue to rely on intermediate nodes (such as routers, base stations, servers, data banks, etc) to store and relay information transmitted from one user (Alice) to another (Bob) especially via social media networks. Every such transmission leaves the original information somewhere on the trail. Millions of personal accounts can be hacked and their personal information can be laid bare for potential abuse. For that reason, end-to-end security over Internet is highly desirable for personal as well as institutional and national security needs.

To ensure end-to-end security, Alice and Bob must share a secret that is not known to anyone else. And this secret should not be decided by a third party (including "administrators" of a network). And Alice and Bob must establish this secret solely by themselves. The next question is: how can they achieve this without inconvenient physical contact? Or how can they achieve this whenever they are within each other's radio range?

The above is just one of many practical applications where reliable and secure transmission of information is highly desired. Wireless transmission of secret (without a prior shared secret) is the primary objective addressed in the field of physical layer security [1]-[17]. This field has grown rapidly especially in the past decade. Many ideas such as beamforming, artificial noise, cooperative node, etc. have been proposed and studied extensively in the literature. Various assumptions such as whether Alice/Bob know or partially know the channel at eavesdropper (Eve) and whether Alice/Bob know or partially know the location of Eve have been used to frame problems to be addressed. However, very limited attention has been devoted to the situation where Eve may have an unlimited number of antennas and be located at an arbitrary location unknown to Alice/Bob.

For strong security, it is desirable to guarantee a positive secrecy against Eve regardless of Eve's number of antennas and Eve's signal-to-noise-ratio (SNR). This is feasible by exploiting the reciprocal channel-state-information (CSI) between Alice and Bob. It is shown in [1] that for each CSI coherence period the achievable information-theoretical secrecy, unconditional on Eve's channel condition (such as Eve's antennas and SNR), equals the entropy $H(S)$ of the (discrete) CSI shared by Alice and Bob. We can refer to $H(S)$ as the strict amount of (achievable) unconditional secrecy (UNS) per coherence period. However, $H(S)$ is generally limited for each coherence period of length K_c, and the strict rate in bits/s/Hz of UNS reduces to zero as K_c increases.

In this paper, we introduce a transmission scheme called randomized reciprocal channel modulation (RRCM) for wireless channels with large K_c. RRCM makes it computationally complex for Eve to obtain user's CSI that is used by transmitter to scramble (and hence is needed by receiver to decode) the information symbols. Subject to Eve's failure to overcome this physical layer complexity, RRCM can achieve a virtually constant (significant) rate of UNS for any large K_c. RRCM is a physical layer encryption method aimed for large K_c unlike all prior methods such as [17].

II. A SIMPLE RRCM SCHEME

Consider a SISO user channel between two half-duplex users where Alice plans to transmit secret information to Bob subject to eavesdropping by Eve with any number of antennas, any noise level and located anywhere (except a fraction of wavelength away from each user). See Fig. 1. We assume that the environment is multipath rich like all terrestrial based radio channels.

Let the channel coherence time be K_c (measured in number of samples in baseband). In coherence period 1, let Bob first

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

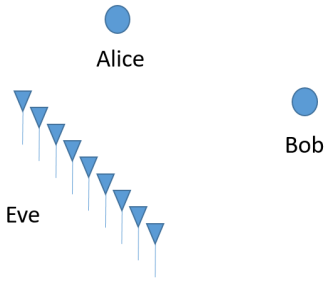

Fig. 1. Achieving a virtually constant (significant) rate of unconditional secrecy against eavesdropper who may have any number of antennas and any noise level.

transmit a pure (publicly known) pilot $p(n)$ so that Alice can estimate the reciprocal channel gain h_1 between Alice and Bob. (At the same time, we know that Eve can obtain its receive channel vector $\mathbf{g}_{B,1}$ with respect to Bob.) This step is similar to a prior idea widely known [13], [14], [15], [16].

After that, we let Alice transmit a sequence of randomized pilots as follows:

$$m_{1,1}p(n), m_{1,2}p(n), \cdots, m_{1,S}p(n) \tag{1}$$

where $m_{1,s}$ for all $s = 1, \cdots, S$ are random complex factors generated by Alice. Then, Bob can perform channel estimation to obtain $h_1 m_{1,s}$ for all s. Note that Alice also knows $h_1 m_{1,s}$ for all s, and Eve can obtain $\mathbf{g}_{A,1} m_{1,s}$ for all s where $\mathbf{g}_{A,1}$ is Eve's receive channel vector with respect to Alice.

The above process is repeated in channel coherence periods 2, 3 and 4. Somewhere within period 4, both Alice and Bob have now obtained $h_1 m_{1,s}, h_2 m_{2,s}, h_3 m_{3,s}, h_4 m_{4,s}$ for $s = 1, \cdots, S$, and they can both compute the following SVD

$$\begin{bmatrix} h_1 m_{1,s} & h_2 m_{2,s} \\ h_3 m_{3,s} & h_4 m_{4,s} \end{bmatrix} = \sigma_{1,s}\mathbf{u}_{1,s}\mathbf{v}_{1,s} + \sigma_{2,s}\mathbf{u}_{2,s}\mathbf{v}_{2,s}. \tag{2}$$

Alice also needs to choose a random complex number from the above SVD. One such choice is

$$\bar{m}_s = \sigma_{1,s} e^{j\mu_{1,s}} \tag{3}$$

where $\mu_{1,s}$ is a random phase which can be chosen to be the phase of the first element of $\mathbf{u}_{1,s}$. Note that Alice can choose $\bar{m}_s$ for all s with any desired property and all other components of the above SVD randomly, and then choose the corresponding $m_{1,s}, m_{2,s}, m_{3,s}, m_{4,s}$ for all s. But Bob must (and can) determine $\bar{m}_s$ for all s from the knowledge of $h_1 m_{1,s}, h_2 m_{2,s}, h_3 m_{3,s}, h_4 m_{4,s}$.

Alice and Bob also need to pre-agree upon how to normalize the phases of the computed singular vectors of SVD, which is an easy task (for example, set the phase of the first element of $\mathbf{v}_{i,s}$ to be zero). All estimation errors by Alice and Bob are assumed to be small (with $\sigma_{1,s} > \sigma_{2,s}$) and can be lumped into the additive noise in the signal received by Bob corresponding to the information symbols transmitted by Alice.

By now, Eve (neglecting its noise) also knows $\mathbf{g}_{A,1} m_{1,s}, \mathbf{g}_{A,2} m_{2,s}, \mathbf{g}_{A,3} m_{3,s}, \mathbf{g}_{A,4} m_{4,s}$ for all s, from which Eve can compute (via a common subspace of $\mathbf{g}_{A,i} m_{i,s}$ for all s and each i) $\hat{m}_{i,s} = g_i m_{i,s}$ for all i and all s where g_i is an ambiguity factor unknown to Eve. The left-hand-side matrix of (2) is equivalent to

$$\begin{bmatrix} h_1 m_{1,s} & h_2 m_{2,s} \\ h_3 m_{3,s} & h_4 m_{4,s} \end{bmatrix} = \begin{bmatrix} \frac{h_1}{g_1}\hat{m}_{1,s} & \frac{h_2}{g_2}\hat{m}_{2,s} \\ \frac{h_3}{g_3}\hat{m}_{3,s} & \frac{h_4}{g_4}\hat{m}_{4,s} \end{bmatrix} \tag{4}$$

where $\frac{h_i}{g_i}$ for all i have the same amount of ambiguity to Eve as h_i for all i. Since $\frac{h_i}{g_i}$ for each i is unknown to Eve, Eve is unable to determine any $\bar{m}_s$ from its knowledge of $\hat{m}_{i,s}$.

With $\bar{m}_s$ for all s in period 4, Alice transmits the following within the rest of period 4:

$$p(n), \bar{m}_1 c_1, \bar{m}_2 c_2, \cdots, \bar{m}_S c_S \tag{5}$$

where c_s for all s are information symbols. Corresponding to the pure pilot $p(n)$ in the above string of symbols, Bob can estimate h_4. Corresponding to $\bar{m}_s c_s$ in the above, Bob receives

$$y_{B,s} = h_4 \bar{m}_s c_s + w_{B,s} \tag{6}$$

where $w_{B,s}$ is the noise (including all perturbations due to channel estimation errors as mentioned before). Since Bob knows $h_4 \bar{m}_s$, Bob can estimate and detect the digital information in c_s for all s. Clearly, the above signal model is equivalent to the output of a fast-fading channel but with all fading parameters known in advance to the transmitter (Alice) and the receiver (Bob).

In parallel to what Bob has done, Eve can estimate $\mathbf{g}_{A,4}$ (which does not help reducing its ambiguity of h_4 due to multipath) and receives

$$\mathbf{y}_{E,s} = \mathbf{g}_{A,4} \bar{m}_s c_s + \mathbf{w}_{E,s} \tag{7}$$

for all s, where $\bar{m}_s$ is unknown to Eve. Since $\bar{m}_s$ for all s are chosen by Alice in a random fashion to completely mask the information in c_s for all s, Eve is made completely blind to the information in c_s.

Consequently, the information transmitted from Alice to Bob is in unconditional secrecy from Eve (unconditional on Eve's number of antennas and noise level). The above process in period 4 can be repeated in period 5 and beyond. The elements in h_1, h_2, h_3, h_4 should be updated accordingly. For example, in period 5, we can replace them by h_2, h_3, h_4, h_5. For the SISO case, there is an initial overhead of three coherence periods. This overhead becomes negligible after a large number of periods.

III. Eve's Challenge to Estimate User's CSI

The previous discussion shows that as long as Eve is unable to find the user's CSI parameters $\mathbf{h} \doteq [h_1, h_2, h_3, h_4]^T$ (or equivalently $\mathbf{h}' \doteq [\frac{h_1}{g_1}, \frac{h_2}{g_2}, \frac{h_3}{g_3}, \frac{h_4}{g_4}]$), Eve is unable to compute $\bar{m}_s$ and hence unable to detect any information from Alice while the data rate from Alice to Bob can be kept at a (significant) positive value over half of period 4 and each of the periods afterwards (and this rate increases as the allocated transmitted power increases).

One should wonder whether Eve is able to have a good estimate of $\mathbf{h}$ if Eve happens to have guessed correctly the digital symbols c_s for $s = 1, \cdots, S_0$. Once Eve had a good estimate of $\mathbf{h}$, Eve would be able to detect the information in

c_s for $s > S_0$ which would mean that not all information in c_s for all s is in unconditional secrecy against Eve.

Next, we show that it is computationally complex for Eve to obtain a consistent estimation of $\mathbf{h}$. Assume that Eve has guessed c_s for $s = 1, \cdots, S_0$ correctly and consequently (ignoring Eve's noise) obtained $\bar{m}_s$ for $s = 1, \cdots, S_0$. To obtain $\bar{m}_s$ for $s > S_0$ (in order to decode c_s for $s > S_0$), Eve must now find $\mathbf{h}$ using $\bar{m}_s$ for $s = 1, \cdots, S_0$.

If Eve applies the following equations that govern (part of) the SVD in (2):

$$\mathbf{H}_s \mathbf{v}_{1,s} = \sigma_{1,s} \mathbf{u}_{1,s} \tag{8}$$

where $\|\mathbf{v}_{1,s}\| = 1$, $\|\mathbf{u}_{1,s}\| = 1$, and $\mathbf{H}_s$ is the matrix on the right of (4), and $s = 1, \cdots, S_0$, then the total number of real-valued unknowns in these equations is $2 \times 4 + 2 \times 2 \times S_0 + 2 \times 2 \times S_0 - 2 \times S_0 = 8 + 6S_0$ where we have counted $\mathbf{h}$, $\mathbf{v}_{1,s}$, $\mathbf{u}_{1,s}$ and two known phases for each s. But the total number of real-valued equations/constraints is $2 \times 2 \times S_0 + 2 \times S_0 = 6S_0$ where we have counted (8) and the norm constraints of $\mathbf{v}_{1,s}$ and $\mathbf{u}_{1,s}$ for all s. We see that the number of unknowns to Eve is always larger than the number of equations/constraints available to Eve. Therefore, using the above method, Eve is unable to obtain a consistent estimation of the user's CSI $\mathbf{h}$.

Now consider that Eve applies all equations in (2). In this case, one can verify that the number of real unknowns is $N_{unk} = 8 + 6S_0$ and the number of real equations is $N_{equ} = 8S_0$. For $N_{unk} \leq N_{equ}$, Eve must choose $S_0 \geq 4$ and hence $N_{unk} \geq 32$. The SVD equations are nonlinear. If brute force is used to search for $\mathbf{h}$, the complexity is $\mathcal{O}(N_q^8)$ where N_q is the number of quantization levels of each real freedom in $\mathbf{h}$. If Newton's algorithm is used, the complexity of each iteration is $\mathcal{O}(N_{unk}^3)$. There is also an issue of incorrect local solutions for Eve due to nonlinearity.

IV. A Principle behind the Choice of Random Modulation

From the previous analysis, we see that Eve's challenge to perform consistent estimation of user's CSI even if Eve has guessed many symbols correctly is because of the following (abstracted) principle. With user's CSI or any critical part of it, denoted by C, Alice applies random attachments A_s for $s = 1, \cdots, S$ and produce at least two inter-dependent components $C_{1,s}$ and $C_{2,s}$ for each s where $C_{1,s}$ is a function of A_s, C and $C_{2,s}$, denoted by $C_{1,s} = f(A_s, C, C_{2,s})$.

The transmission scheme must also make sure that Bob is also able to obtain $C_{1,s}$ for all s while Eve is denied the ability to obtain or compute any of $C_{1,s}$.

Alice applies $C_{1,s}$ (which could be a matrix) to protect the information symbol c_s (which could be a vector) via modulation while Bob is able to demodulate $C_{1,s}$ to retrieve all information from c_s for all s.

In this way, even if Eve has obtained A_s for all s due to channel training between Alice and Bob, and has guessed correctly c_s for some s and consequently obtained $C_{1,s}$ for some s, Eve's knowledge about C is

$$C_{1,s} = f(A_s, C, C_{2,s}) \tag{9}$$

for some s, where C and $C_{2,s}$ are still unknown to Eve. Ideally, we would like the number of unknowns to Eve to be always larger than the number of equations available to Eve. But the previous example does not meet this requirement.

It is important to note that the function $f(A_s, C, C_{2,s})$ must be such that it cannot be degenerated into any form that reduces the effective number of variables. For example, we cannot allow $f(A_s, C, C_{2,s}) = f'(A_s, g(C, C_{2,s}))$ where C and $C_{2,s}$ are effectively lumped into $g(C, C_{2,s})$. The methods for designing $f(A_s, C, C_{2,s})$ are not yet well developed. The previous example shown in (2) is based on SVD.

V. For SIMO User Channel

For a SIMO user channel from Alice to Bob, we have the following signal model

$$\mathbf{y}_B(n) = \mathbf{h}_B x_A(n) + \mathbf{w}_B(n) \tag{10}$$

where $\mathbf{h}_B$ is the $N_B \times 1$ channel vector from Alice to Bob. With channel reciprocal property, we have

$$y_A(n) = \mathbf{h}_B^T \mathbf{x}_B(n) + \mathbf{w}_A(n) \tag{11}$$

where $\mathbf{x}_B(n)$ is the transmitted vector from Bob.

If $N_B = 2$, the previous SISO RRCM method can be applied here over two channel coherence periods. In period 1, Bob first sends an orthogonal pilot matrix, e.g.,

$$[\mathbf{x}_B(1), \mathbf{x}_B(2)] = \sqrt{P_T} \mathbf{I}_{N_B} \tag{12}$$

and then Alice obtains $\mathbf{h}_{B,1}$. Alice then sends the random symbols $m_{1,1}, \cdots, m_{1,S}$ and $m'_{1,1}, \cdots, m'_{1,S}$ at the power P_T so that Bob obtains $\mathbf{h}_{B,1} m_{1,s}$ and $\mathbf{h}_{B,1} m'_{1,s}$ for all s.

In period 2, a similar process is repeated. Hence, Alice and Bob each knows $\mathbf{h}_{B,i} m_{i,s}$ and $\mathbf{h}_{B,i} m'_{i,s}$ for $i = 1, 2$ and all s. Like (2), the following SVD can be computed by Alice/Bob:

$$\begin{bmatrix} \mathbf{h}_{B,1} m_{1,s} & \mathbf{h}_{B,1} m'_{1,s} \\ \mathbf{h}_{B,2} m_{2,s} & \mathbf{h}_{B,2} m'_{2,s} \end{bmatrix} = \sum_{i=1}^{2} \sigma_{i,s} \mathbf{u}_{i,s} \mathbf{v}_{i,s}^H \tag{13}$$

from which a random factor $\bar{m}_s$ is chosen for each s. (For Alice, $\bar{m}_s$ can be decided before $m_{i,s}$ and $m'_{i,s}$ for $i = 1, 2$ are chosen.)

For the rest of period 2, Alice transmits a packet similar to that in (5). This way, Bob can receive all the information from Alice reliably.

The situation for Eve is similar to the SISO case. Although in theory Eve can obtain $\mathbf{h}_{B,1}$ and $\mathbf{h}_{B,2}$ from a finite number of correctly guessed information symbols transmitted from Alice, it is costly for Eve to do so.

If $N_B \geq 4$, a similar scheme can be devised where in period 1, both channel estimation and information transmission can be conducted so that there is no initial overhead of coherence periods as needed for the SISO case.

VI. For MISO User Channel

Now assume that Alice has $N_A = n_A^2 \geq 4$ antennas and Bob has a single antenna. In any given coherence period, Bob can first send a pure pilot so that Alice obtains the $N_A \times 1$ channel vector $\mathbf{h}_A$. Alice then follows by transmitting

$$\sqrt{P_T} \mathbf{I}_{N_A}, \sqrt{P_T} \mathbf{D}_1 \mathbf{I}_{N_A}, \cdots, \sqrt{P_T} \mathbf{D}_S \mathbf{I}_{N_A} \tag{14}$$

where $\mathbf{D}_s = diag[m_{s,1}, \cdots, m_{s,N_A}]$ with random diagonal elements. Consequently, Bob can obtain the following from its received signal:

$$\mathbf{h}_A, \mathbf{D}_1\mathbf{h}_A, \cdots, \mathbf{D}_S\mathbf{h}_A. \tag{15}$$

Within the remaining of the current coherent period, Alice transmits the following information carrying symbols via the best antenna (which should be concatenated or interleaved with the randomized pilots in (14) for best carrier and symbol synchronization)

$$\sqrt{P_T}\bar{m}_1 c_1, \cdots, \sqrt{P_T}\bar{m}_S c_S \tag{16}$$

where $\bar{m}_s$ is a random complex scalar which can be computed from the following SVD

$$\mathbf{H}_{s,MISO} = \sum_{i=1}^{n_A} \sigma_{i,s}\mathbf{u}_{i,s}\mathbf{v}_{i,s}^H \tag{17}$$

with $\mathbf{H}_{s,MISO}$ being a $n_A \times n_A$ matrix consisting of the elements in $\mathbf{D}_s\mathbf{h}_A$.

Similar to the SISO case, we can choose $\bar{m}_s = \sigma_{1,s}e^{j\mu_{1,s}}$ with $\mu_{1,s}$ being the phase of the first element of $\mathbf{u}_{1,s}$ (and the phase of the first element of $\mathbf{v}_{1,s}$ set to zero). Alice can choose $\bar{m}_s$ for all s first (to ensure sufficient randomness) before choosing $\mathbf{D}_s$ for all s (corresponding to random choices of all other components in (17) besides $\bar{m}_s$).

It is easy to verify that Bob can detect all the information from Alice reliably provided that the data rate in c_s from Alice is less than the capacity of the following equivalent SISO "fast-fading" channel:

$$y_{B,s} = \sqrt{P_T}h_{max}\bar{m}_s c_s + w_{B,s} \tag{18}$$

where $s = 1, \cdots, S$ and $w_{B,s}$ contains all the perturbations due to channel estimation errors by Alice and Bob.

Eve with two or more antennas and negligible noise can obtain $\bar{m}_s c_s$. Without knowing $\bar{m}_s$, Eve is unable to decode all information in c_s. To obtain $\bar{m}_s$ for all s, Eve must know some c_s. If Eve has guessed c_s for $s = 1, \cdots, S_0$ correctly with $S_0 \geq N_A$, Eve can possibly compute $\mathbf{h}_A$ at a high computational cost (similar to the SISO case). Unless Eve can overcome this physical layer complexity, all the information from Alice is protected from Eve.

VII. For SISO OFDM System

We now apply the SISO RRCM scheme shown in section II to a multicarrier or orthogonal frequency division multiplexing (OFDM) system. Assume that in the time domain, the input-output of the SISO (wideband) channel from Alice to Bob is governed by

$$y_B(n) = \sum_{l=0}^{L} h(l)x_A(n-l) + w_B(n) \tag{19}$$

where $h(l), l = 0, \cdots, L$, is the channel impulse response of at least $L_0 + 1 \leq L + 1$ nonzero (initial and incoherent) samples. In other words, $L_0 + 1$ and $L + 1$ are the lower and upper bounds on the length of $h(l)$. Also assume that $L_0 + 1 \geq 4$.

For any coherent period, Bob first transmits a pilot $p(n) = \sqrt{P_T}\delta(n)$ and Alice then obtains the reciprocal channel impulse response $h(n)$ and hence its N-point Fast Fourier transform (FFT) $H(k)$ for $k = 0, \cdots, N-1$ with $N = 2^p = q(L_0 + 1) > L$ where p and q are integers. Typically, in practice, $N \gg L$.

Among $H(k)$ for $k = 0, \cdots, N-1$, these samples $H(i), H(i+q), \cdots, H(i+L_0q)$ for each $i = 0, \cdots, q-1$ are incoherent. Each segment (sth segment) of the OFDM packet from Alice has a section of randomized pilots from concatenation of the q rows of the following matrix

$$\begin{matrix} \sqrt{P_T}m_{0,0,s}, \mathbf{0}_L^T, & \cdots, & \sqrt{P_T}m_{0,3,s}, \mathbf{0}_L^T, \\ \cdots, & \cdots, & \cdots, \\ \sqrt{P_T}m_{q-1,0,s}, \mathbf{0}_L^T, & \cdots, & \sqrt{P_T}m_{q-1,3,s}, \mathbf{0}_L^T \end{matrix} \tag{20}$$

which is followed by a L-sample prefixed IFFT of a $N \times 1$ vector from concatenation of the $L_0 + 1$ rows in the following matrix

$$\begin{matrix} \bar{m}_{0,s}c_{0,s}, & \bar{m}_{1,s}c_{1,s}, & \cdots, & \bar{m}_{q-1,s}c_{q-1,s}, \\ \bar{m}_{0,s}c_{q,s}, & \bar{m}_{1,s}c_{q+1,s}, & \cdots, & \bar{m}_{q-1,s}c_{2q-1,s}, \\ \cdots & \cdots & \cdots & \cdots \\ \bar{m}_{0,s}c_{qL_0,s}, & \bar{m}_{1,s}c_{qL_0+1,s}, & \cdots, & \bar{m}_{q-1,s}c_{q(L_0+1)-1,s} \end{matrix} \tag{21}$$

In (20), $\mathbf{0}_L^T$ denotes L zero samples, $\bar{m}_{i,s}$ for each $i = 0, \cdots, q-1$ and s is a random complex factor chosen from the following SVD

$$\mathbf{H}_{s,OFDM,i} = \sum_{k=1}^{2} \sigma_{k,s,i}\mathbf{u}_{k,i,s}\mathbf{v}_{k,i,s}^H \tag{22}$$

where $\mathbf{H}_{s,OFDM,i}$ is a 2×2 matrix consisting of $H(i)m_{i,0,s}, H(i+q)m_{i,1,s}, H(i+2q)m_{i,2,s}, H(i+3q)m_{i,3,s}$.

For each segment of the OFDM packet, the ratio of the number of information symbols over the number of pilot-plus-information symbols is $\frac{q(L_0+1)}{q(L_0+1)+L+4q(L+1)}$ which is approximately $\frac{L_0+1}{L_0+1+4(L+1)}$ for large q. The best situation is when $L_0 = L$ where the ratio is $\frac{1}{5}$. This is a loss of symbol rate in comparison to the conventional OFDM system where the ratio is $\frac{N}{N+L} \approx 1$. But this loss of symbol rate has helped to achieve a virtually perfect unconditional secrecy of the information from Alice to Bob.

VIII. Conclusion

This paper has introduced a novel physical layer encryption method called randomized reciprocal channel modulation (RRCM), which allows a virtually constant (significant) rate R_{UNS} of unconditional secrecy (UNS) for wireless transmission of information against Eve with any number of antennas, any location (a fraction of wavelength away from each user in multipath environment) and any noise level, regardless of how large the channel coherence time and/or bandwidth may be. This rate R_{UNS} is subject to Eve's failure to overcome a high computational complexity at the physical layer caused by RRCM. This eavesdropping complexity is much higher than those of prior methods such as transmit-beamforming and artificial-noise schemes. Detailed comparisons will be shown in a future work.

REFERENCES

[1] 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.

[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] 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.

[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] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550-1573, 3rd Quart., 2014.

[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun. Mag., vol. 53, pp. 20-27, Apr. 2015.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," Proceedings of the IEEE, Vol. 104, No. 9, September 2016.

[9] X. Chen, D. W. K. Ng, W. Gerstacker, and H.-H. Chen, "A survey of multiple-antenna techniques for physical layer security," IEEE Commun. Surveys Tutorials, vol. 19, pp. 1027-1053, Jun. 2017.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive MIMO," IEEE Transactions on Information Theory, Vol. 63, No. 8, pp. 5419-5436, Aug. 2017.