Evaluation of Physical Layer Secrecy in MIMO Ultra-Wideband System using Time-Reversal Techniques

Vu Trong Tan, Dac-Binh Ha, *Member, IEEE*, Duc-Dung Tran
Research and Development Center, Duy Tan University, Danang, Vietnam
E-mail: vutrongtan@live.com, hadacbinh@duytan.edu.vn, dung.td.1227@gmail.com

***Abstract*—Physical layer secrecy in wireless communication is a new approach of information security and has emerged into a fascinating topic attracting lots of research. Ultra-WideBand (UWB) technology in conjunction with Time-Reversal (TR) is used to improve the speed of transmission and reduce the cost and complexity for the receiver. This paper focuses on the evaluation of physical layer secrecy in Multi-Input Multi-Output (MIMO) UWB system with TR and compares to the system without using TR technique to clarify the advantages of this technique. Simulation results show that the secrecy capacity of UWB system is significantly improved when applying TR technique.**

***Index Terms*—physical layer secrecy, UWB, time reversal, secrecy capacity.**

I. Introduction

In current wireless networks, most of the security systems use security mechanisms based on complex calculations on the assumption that the eavesdroppers have limited computing capability and a lack of efficient algorithms. However, this assumption is not convincing because of the rapid development of modern computers (such as quantum computers) as well as high-performance algorithms. Moreover, the traditional security was made at a higher layer, normally in the application layer (APP) with the assumption that the physical layer (PHY) was established with no error [1]. With the appearance of ad-hoc networks and hierarchical networks [2], the techniques of APP layer, such as encoding, are too complex and difficult to implement. In addition, using authentication and encoding in security mechanisms at the APP layer not only creates transmission latency and high power consumption but also reduces system capacity due to the overload of computation and signal [3]. As a result, the security technique based on the computational complexity is inconsistent with wireless networks and large-scale random or inconsistent with the hierarchical network and networks that require stringent security and time. Thus, there have been numerous research studies conducted recently on the basic ability of the PHY to improve the security of wireless networks. The researchers have recently focused on information security issues at the physical layer in three main approaches: key-based secrecy [4], [5], [6], [7], key-less security [8], [9], [10], and methods of evaluating security at the physical layer [11], [12], [13]. In the last one, a system is called having potentiality to ensure the security of information when the legitimate channel capacity is greater than the eavesdropper's channel capacity. The introduced concept of secrecy capacity is the deviation between the legitimate channel capacity and the eavesdropper's channel capacity. A system is considered capable of ensuring high safety information if the secrecy capacity is large and this is viewed as a key indicator to evaluate the performance of the security of the system.

In this paper, we chose UWB systems to implement. UWB technology is a promissing research direction in recent years because of its capability in high-speed communication over a short distance [9], [10], [14], [15]. UWB technology effectively solves the problems of bandwidth limit in wireless environments [16]. However, it is realized that channels in reality are multi-path fading channels, so problems affecting quality of transmission in UWB systems serving multi-users (MU) are really complex. We can resolve these problems by combining UWB systems and the time reversal technique to improve the transmission rate and minimize the influences of channels thus increasing the quality of UWB systems [10], [17].

In [10], the authors give the results related to the channel capacity of MIMO UWB TR MU system with environmental conditions having correlation between the antenna. In addition, in paper [18], the authors have shown that the channel capacity of the UWB system in case using the TR technique is higher than not apply TR one. Moreover, the TR technique shows good performance when operating in high noise environment. Currently, the level of security in UWB systems are developing shared a secret key between the base station and the receiver from which to establishing a secure channel [19].

To the best of our knowledge, there has been no previous work that mentioned evaluating the secrecy capacity of the UWB system consisting of a couple of multi-antennas devices, in the presence of a multi-antennas passive eavesdropper over Rayleigh fading channel. Therefore, in this paper, we focus on evaluating information secrecy capabilities at the physical layer of the UWB systems applying the TR techniques base on a secrecy capacity, compared with the system not applicable the TR technique to clarify the advantages of this technique.

The rest of this paper is organized as follows: Section II introduces the system model, Section III presents the secrecy capacity of UWB-TR system, Section IV gives simulation results on the capacity of the system model and we conclude our discussions in Section V.

978-1-4799-2903-0/14/$31.00

II. System model

We consider system model as Fig. 1, includes a transmitter Alice and a receiver Bob, at the same time presence of the eavesdropper Eve in Rayleigh fading environment. Eve is passive eavesdropping machine trying to extract information from Alice to Bob without active attacks. The system is studied UWB MIMO system, i.e.. the transmitter and the receiver (Bob, Eve) are using multiple antennas.

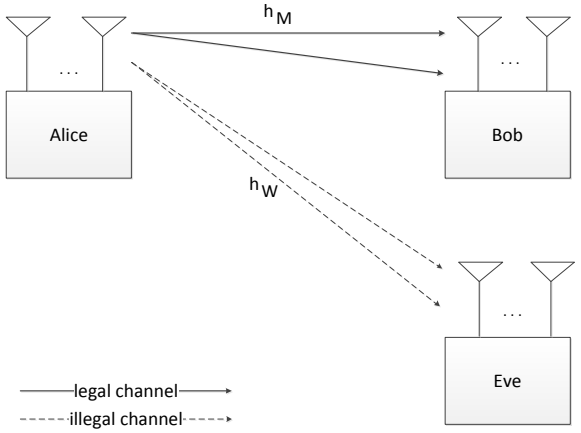

Figure 1. MIMO UWB system model

Alice transmits to Bob via data channel (denoted as M), however due to the nature of the wireless communication channel, this data is also received by the eavesdropper Eve via eavesdropping channel (denoted as W). In this paper, we do not consider the correlation of transmit antennas and receive antennas. We suppose that the number of transmitting antennas is M_T and the number of Bob's antennas is M_{R_b}, the number of Eve's antennas is M_{R_e}.

The signal obtained at Bob is [18]:

$$\mathbf{Y}_M = \mathbf{H}_\mathrm{M}\mathbf{X} + \mathbf{n}_M, \tag{1}$$

where: $\mathbf{Y}_\mathrm{M}$ is the matrix of received signals at the user; $\mathbf{X}$ is the matrix of transmitted signals; $\mathbf{n}_M$ is the white Gaussian noise at Bob; $\mathbf{H}_\mathrm{M}$ is the matrix of channel impulse responses (CIRs) of environmental between Alice and Bod with dimension $M_{R_b}\times M_T$:

$$\mathbf{H}_\mathrm{M} = \begin{bmatrix} h_{11} & h_{12} & \cdots & \mathrm{h}_{1M_T} \\ h_{21} & h_{22} & \cdots & h_{2M_T} \\ \vdots & \vdots & \ddots & \vdots \\ h_{M_{R_b}1} & \mathrm{h}_{M_{R_b}2} & \cdots & h_{M_{R_b}M_T} \end{bmatrix}, \tag{2}$$

where, h_{ij} is the CIR between the $j-th$ transmit antenna and the $i-th$ receive antenna of the user.

It is represented as:

$$h_{ij}(t) = \sum_{l=0}^{L_1-1} \alpha_l^{ij}\delta(t-\tau_l^{ij}), i = 1, \cdots, M_{R_b}; j = 1, \ldots, M_T, \tag{3}$$

with $\alpha_l^{ij}$and $\tau_l^{ij}$are the amplitude and the delay of the$-th$ tap, respectively.

The discrete time form of is expressed as:

$$h_{ij}[k] = [h_{ij}[0]\ h_{ij}[1]\ ...\ h_{ij}[L_1-1]], \tag{4}$$

where $h_{ij}[k]$, $k = 0, \ldots, L_1-1$ is the $k-th$ tap of CIR with the length of L_1.

For each downlink, we assume that the corresponding amplitude component α_l^{ij} is modeled as a Rayleigh random variable whose probability density function (PDF) is [20]

$$f_{\alpha_l}(x) = \frac{x}{\sigma_l^2} e^{-\frac{x^2}{2\sigma_l^2}},\ 0 \le l \le L_1-1, \tag{5}$$

Channel capacity of the MIMO UWB system of user will be calculated by the following formula [15]:

$$C_M = \log_2(\det(\mathbf{I}_{M_{R_b}} + SNR_M \mathbf{H}_\mathrm{M}\mathbf{H}_\mathrm{M}^\mathbf{H})), \tag{6}$$

where $\mathbf{I}_{M_{R_b}}$is the unix matrix with demension $M_{R_b}\times M_{R_b}$, SNR_M is the signal to noise of legal and

$$\mathbf{H}_\mathrm{M}^\mathbf{H} = \begin{bmatrix} h_{11}^* & h_{12}^* & \cdots & \mathrm{h}_{1M_T}^* \\ h_{21}^* & h_{22} & \cdots & h_{2M_T}^* \\ \vdots & \vdots & \ddots & \vdots \\ h_{M_{R_b}1}^* & \mathrm{h}_{M_{R_b}2}^* & \cdots & h_{M_{R_b}M_T}^* \end{bmatrix}, \tag{7}$$

With h_{ij}^* is complex conjugate of $h_{ij},\ i = 1, \ldots, M_{R_b},\ j = 1, \ldots, M_T$.

Similarly, the received signal at the eavesdropper has the following form:

$$\mathbf{Y}_W = \mathbf{H}_\mathrm{W}\mathbf{X} + \mathbf{n}_W, \tag{8}$$

So the channel capacity of the MIMO UWB system of eavesdropper will be:

$$C_W = \log_2(\det(\mathbf{I}_{M_{R_e}} + SNR_W \mathbf{H}_\mathrm{W}\mathbf{H}_\mathrm{W}^\mathbf{H})), \tag{9}$$

with $\mathbf{I}_{M_{R_e}}$is the unix matrix with demension $M_{R_e}\times M_{R_e}$, SNR_W is the signal to noise of illegal and $\mathbf{H}_\mathrm{W}^\mathbf{H}$is the matix complex conjugate of $\mathbf{H}_\mathrm{W}$.

III. Secrecy capacity of the MIMO UWB-TR system

Secrecy capacity is the deviation between the capacity of the main channel and the capacity of the eavesdropping channel [21]. A system is considered capable of ensuring high safety information if the secrecy capacity is positive.

We consider the MIMO UWB systems as Fig. 2. The difference between UWB and UWB TR systems is that, UWB TR systems only operate when it anticipates the CIRs' information forwarded each user. Therefore, in UWB TR systems, first of all, intended users will send an impulse to transmitters,

the received signal form at transmitter is CIRs formed of that environment. When the transmitter received CIRs information from the users, the block Time Reversal (TR) Mirror will use these information of CIRs to create waveforms which are used for communication between transmitter and intended users [22].

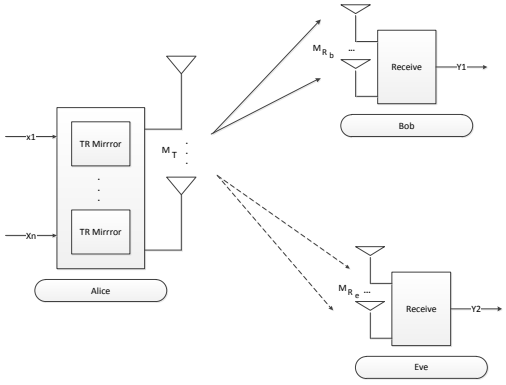

Figure 2. The MIMO UWB TR system model

Let $\mathbf{G}$ is TR Mirror's matrix, which is expressed as:

$$\mathbf{G_M} = \begin{bmatrix} g_{11} & \mathrm{g}_{12} & \cdots & g_{1M_{R_b}} \\ g_{21} & \mathrm{g}_{22} & \cdots & \mathrm{g}_{2M_{R_b}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{g}_{M_T1} & \mathrm{g}_{M_T2} & \cdots & \mathrm{g}_{M_TM_{R_b}} \end{bmatrix}, \quad (10)$$

where $g_{ij}[k] = h^*_{ij}[L_1 - 1 - k]; i = 1, \ldots, M_T; j = 1, \ldots, M_{R_b}; k = 0, \ldots, L_1 - 1$.

Let $\hat{\mathbf{H}}_\mathrm{M}$ is the equivalent CIRs matrix, which is represented as:

$$\hat{\mathbf{H}}_\mathrm{M} = \mathbf{H}_\mathrm{M} * \mathbf{G}_\mathrm{M} = \begin{bmatrix} \hat{h}_{11} & \hat{h}_{12} & \cdots & \hat{h}_{1\mathrm{M}_{R_b}} \\ \hat{h}_{21} & \hat{h}_{22} & \cdots & \hat{h}_{2\mathrm{M}_{R_b}} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{h}_{M_{R_b}1} & \hat{h}_{M_{R_b}2} & \cdots & \hat{h}_{M_{R_b}\mathrm{M}_{\mathrm{R_b}}} \end{bmatrix}, \quad (11)$$

with $\hat{h}_{ij} = \sum_{m=1}^{M_T} h_{im} * g_{mj}; i, j = 1, \ldots, M_{R_b}$, $\mathbf{H_M}$ come from (2). Thus, equation (1) can rewrite as the following:

$$\mathbf{Y}_M = \hat{\mathbf{H}}_\mathrm{M}\mathbf{X} + \mathbf{n}_M, \quad (12)$$

So, channel capacity of the MIMO UWB TR system is:

$$C_M^{TR} = \log_2(\det(\mathbf{I}_{M_{R_b}} + SNR_M\hat{\mathbf{H}}_\mathrm{M}\hat{\mathbf{H}}_\mathrm{M}^\mathbf{H})), \quad (13)$$

where $\mathbf{I}_{M_{R_b}}$ is the unix matrix with demension $M_{R_b} \times M_{R_b}$, SNR_M is the signal to noise of legal and

$$\hat{\mathbf{H}}_\mathrm{M}^\mathbf{H} = \begin{bmatrix} \hat{h}^*_{11} & \hat{h}^*_{12} & \cdots & \hat{h}^*_{1\mathrm{M}_{R_b}} \\ \hat{h}^*_{21} & \hat{h}^*_{22} & \cdots & \hat{h}^*_{2\mathrm{M}_{R_b}} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{h}^*_{M_{R_b}1} & \hat{h}^*_{M_{R_b}2} & \cdots & \hat{h}^*_{M_{R_b}\mathrm{M}_{\mathrm{R_b}}} \end{bmatrix} \quad (14)$$

With $\hat{h}^*_{ij}$ is complex conjugate of $\hat{h}_{ij},\ i = 1, \ldots, M_{R_b},\ j = 1, \ldots, M_{R_b}$.

Then the instantaneous secrecy capacity is given by [15]:

$$\begin{aligned} C_S &= [C_M - C_W]^+ \\ &= \begin{cases} \log_2(\gamma_M) - \log_2(\gamma_W) & , \gamma_M > \gamma_W \\ 0 & , \gamma_M \le \gamma_W \end{cases} \end{aligned} \quad (15)$$

Where:

$$\gamma_M = \det(\mathbf{I}_{M_{R_b}} + SNR_M\hat{\mathbf{H}}_\mathrm{M}\hat{\mathbf{H}}_\mathrm{M}^\mathbf{H})$$
$$\gamma_W = \det(\mathbf{I}_{M_{R_e}} + SNR_W\mathbf{H}_\mathrm{W}\mathbf{H}_\mathrm{W}^\mathbf{H})$$

Easy to see that the secrecy capacity of information systems is non-negative parameter. Capacity secrecy of information systems is 0 when the capacity of illegal channel greater than the channel capacity of legal channel.

IV. Simulation results

To make this comparison, we simulate the channel capacity of legal channels for UWB MIMO systems in two cases: using TR technique and not using TR technique. Illegal channels in UWB MIMO systems do not use TR techniques. Notice that, we do simulation by using Matlab with the parameters are given in Table I.

Table I
General simulation parameters

Parameters	System values
Environment	Rayleigh
Sampling time of the system (T_S)	$\frac{1}{6}10^{-9}$
Delay spread of the channel (∂_T)	$125T_S$
SNR (dB)	-10dB – 30bB

A diagram of the survey system is described in Fig. 2 Simulation results are showed from Fig. 3 to Fig. 8.

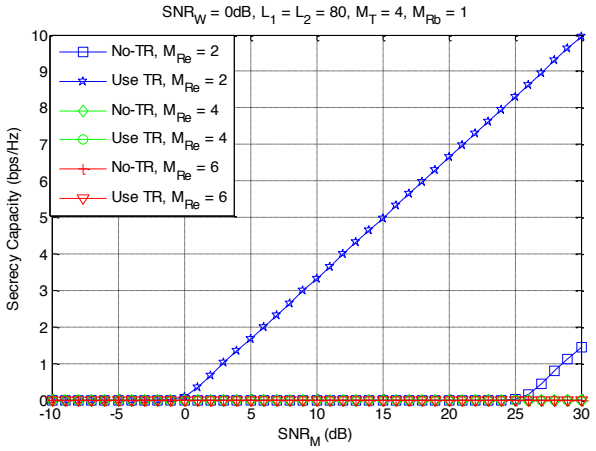

Figure 3. The simulation result when changing the number antenna of illegally channel

Fig. 3 presents the Secrecy capacity (C_S) for different M_{R_e}, L_1, L_2 are length of legal's CIRs and illegal's CIRs, respectively. Assuming $SNR_W = 0dB$, $L_1 = L_2 = 80$, $M_T = 4$ and $M_{R_b} = 1$. In this figure, we observe that, when M_{R_e} increases then C_S decreases and if $M_{R_e} > M_{R_b}$then $C_S \to 0$ even when $SNR_M > SNR_W$. In other words, capacity of illegal channel is more and more better than legal channel's when M_{R_e}increasing. At the same time, we can also observe that, when applying Time Reversal (TR) technique, C_S is much better than that not applying this technique.

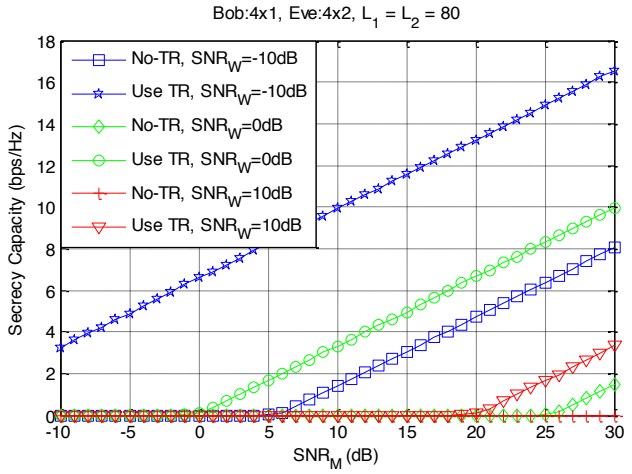

Figure 4. The simulation result when changing the SNR of illegally channels

Fig. 4 presents C_S for different SNR_W, assuming $L_1 = L_2 = 80$, $M_T = 4$, $M_{R_b} = 1$ and $M_{R_e} = 2$. We see that, the higher SNR_M the higher secrecy capacity and the higher SNR_W the lower secrecy capacity. Thus, when SNR_W increases then capacity of illegal channel is more and more better than legal channel's. Moreover, we also have a conclusion similar to Fig. 3 when applying TR technique.

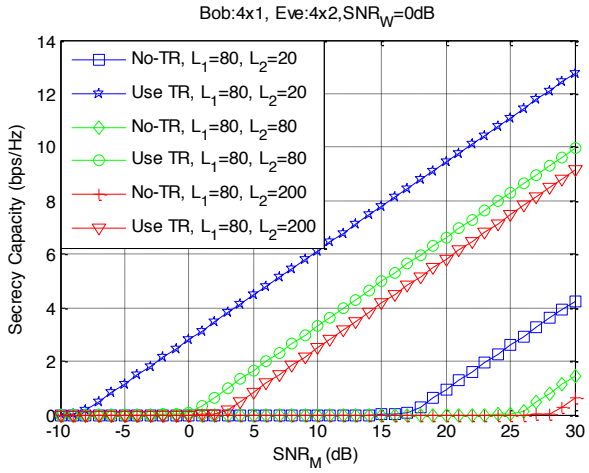

Figure 5. The simulation results when changing numbers of tap receivables in illegally channel

Fig. 5 presents C_S for different L_2, assuming $SNR_W = 0dB$, $L_1 = 80$, $M_T = 4$, $M_{R_b} = 1$ and $M_{R_e} = 2$. When L_2 increases then C_S decreases and vice versa. In other words, capacity of illegal channel is more and more better than legal channel's when L_2 increases. We also clearly observe that this result is much better when applying TR technique.

When we increase M_{R_b} (legal channel is a MIMO system) then aforementioned results are better. This is shown in Fig. 6, Fig. 7 and Fig. 8, respectively.

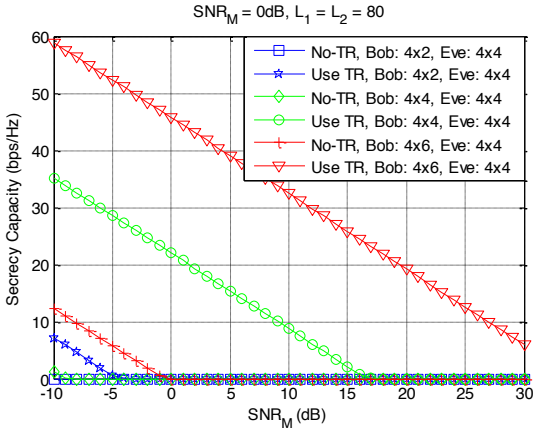

Figure 6. The simulation result when changing the number antenna of illegally channel

Fig. 6 shows the secrecy capacity for different M_{R_b}, assuming $M_{R_e} = 4$, $M_T = 4$, $SNR_W = 0dB$, and $L_1 = L_2 = 80$. We see that, when $M_{R_b} < M_{R_e}$ then C_S increases insignificantly but when $M_{R_b} > M_{R_e}$ then C_S increases more quickly. And this result is much better when applying TR technique. Thus, when M_{R_b} increases then capacity of legal channel is more and more better than illegal channel's.

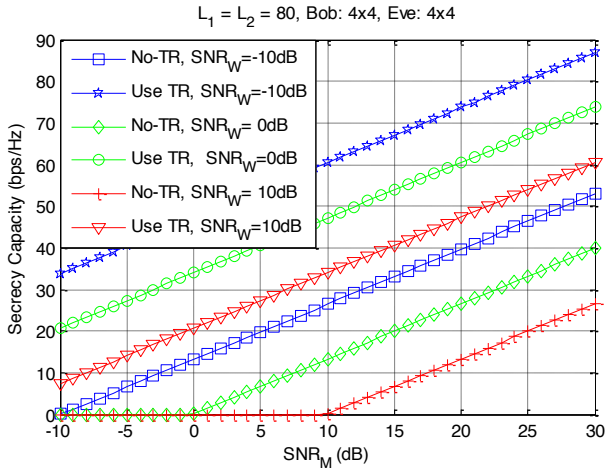

Figure 7. The simulation results when changing the SNR of illegally channels

Fig. 7 shows C_S for different SNR_W, assuming $M_T = M_{R_b} = M_{R_e} = 4$, and $L_1 = L_2 = 80$. In comparison to the results in Fig. 4 (with assuming $M_T = 4$, $M_{R_b} = 1$, $M_{R_e} = 2$ and $L_1 = L_2 = 80$), we see that, the results in Fig. 7 are much better than that in Fig. 4. This also means when SNR_W increases, the increase in M_{R_b} will help to improve secrecy capacity. Moreover, Fig. 7 also shows that, with $M_{R_b} = M_{R_e}$, $L_1 = L_2$, when applying TR technique, $C_S > 0$ even when $SNR_M < SNR_W$.

Similar conclusions can also be obtained when the number of taps of illegal channel (L_2) varies as show in Fig. 8, in which the selected simulation values are $SNR_W = 0dB$, $M_T = M_{R_b} = M_{R_e} = 4$ and $L_1 = 80$.

Thus, the simulation results showed that, secrecy capacity increases when the parameters of legal channel (M_{R_b}, SNR_M and L_1) increase or when the parameters of illegal channel (M_{R_e}, SNR_W and L_2) decrease. Moreover, secrecy capacity will be much better if TR technique is employed.

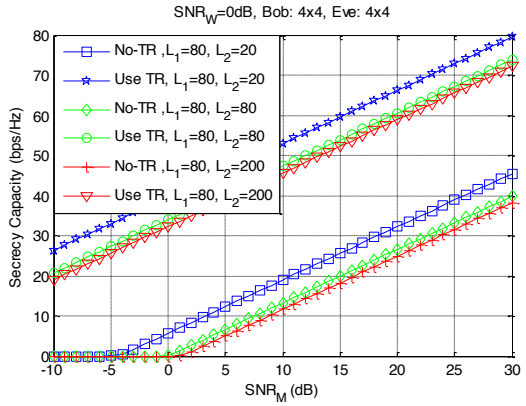

Figure 8. The simulation result when changing the numbers of tap receivables of illegally channel

V. Conclusion

In this paper, we have focused on studying and implementing simulations for secrecy capacity of the MIMO UWB system in the scenarios of the applying and not applying Time Reversal technique. From the study and implementation, the advantages and effectiveness of the combination of UWB systems and TR technique is expected to be seen clearly. The simulation results showed that increased secrecy capacity while increasing numbers of antennas or numbers of taps receivables at legal receiver.

References

[1] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Tech.*, vol. 54(6), pp. 2515–2534, 2008.

[2] M. Debbah, "Mobile flexible networks: the challenges ahead," in *Int. Proc. ATC*, 2008.

[3] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *in Proc. ISIT*, 2005.

[4] U. Maurer, "Secret key agreement by public discussion form common information," *IEEE Trans. Info. Theory*, vol. 39, pp. 733–742, 1993.

[5] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas and Propagation*, vol. 53(11), pp. 3776–3784, 2005.

[6] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *in Proc. CCS*, 2007.

[7] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Info. Forensics Security*, vol. 5(2), pp. 240–254.

[8] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010.

[9] F. Han, Y.-H. Yang, B. Wang, Y. Wu, and L. K.J.R., "Time-reversal division multiple access in multi-path channels," *Global Telecommunications Conference 2011*, pp. 1–5, 2011.

[10] T. H. Vu, N. T. Hieu, H. D. T. Linh, N. T. Dung, and L. V. Tuan, "Channel capacity of multi user TR-MIMO-UWB communications system," in *International Conference on Computing, Management and Telecommunications (ComManTel)*, 2013, pp. 22–26.

[11] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54(8), pp. 1355–1387, 1975.

[12] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24(3), pp. 339–348, 1978.

[13] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info. Theory*, vol. 54(10), pp. 4687–5403, 2008.

[14] H. Nguyen, Z. Zhao, F. Zheng, and T. Kaiser, "Preequalizer design for spatial multiplexing simo-uwb tr systems," vol. 59, no. 8, pp. 3798–3805, 2010.

[15] T. K. Nguyen, H. Nguyen, F. Zheng, and T. Kaiser, "Spatial correlation in the broadcast mu-mimo uwb system using a pre-equalizer and time reversal pre-filter," in *Proc. 4th Int Signal Processing and Communication Systems (ICSPCS) Conf*, 2010, pp. 1–6.

[16] D. P. A. M. M. Di Benedetto, T. Kaiser and I. Opperman, *UWB Communication Systems A Comprehensive Overview*. Hindawi Publising, May, 2006.

[17] R. C. Qiu, C. Zhou, N. Guo, and J. Q. Zhang, "Time reversal with miso for ultrawideband communications: Experimental results," vol. 5, no. 1, pp. 269–273, 2006.

[18] H. T.D.Dung, T.H.Vu, "Applying time-reversal technique for mu mimo uwb communication systems," *The World Congress on Engineering and Computer Science*, 2013.

[19] S. R. Wilson. R, Tse.D, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE International Conference*, pp. 270–275, 2007.

[20] Y.-H. Chang, S.-H. Tsai, XiaoliYu1, and C.-C. J. Kuo, "Performance enhancement of channel-phase precoded ultra-wideband (cpp-uwb) systems by rake receivers," in *IEEE Global Telecommunications Conference*, 2008.

[21] A. Goldsmith, *Wireless Communications*. Cambridge University, 2005.

[22] T. Kaiser and F. Zheng, *Ultra-wideband Systems With MIMO*. Wiley, 2010.