Secure Multiple-Antenna Ultrawideband System: A Wireless Physical-Layer Security Perspective

Tanit Somleewong and Kiattisak Maichalernnukul
(Corresponding author: Kiattisak Maichalernnukul)

College of Information and Communication Technology, Rangsit University
52/347 Phaholyothin Road, Pathumthani 12000, Thailand
(Email: kiattisak.m@rsu.ac.th)
(Received Oct. 12, 2017; revised and accepted Jan. 10, 2018)

Abstract

Recently, it has been suggested that the cryptographic security of wireless communication systems can be improved by exploiting characteristics of ultrawideband (UWB) signals or spatial diversity in multiple-antenna channels. In this paper, a multiple-antenna prerake UWB system which can achieve robust physical-layer security is proposed. The security performance of the proposed system is analytically evaluated in terms of the probability of an adversary correctly determining a secret key versus the decoding error probability of a legitimate receiver. Numerical results based on a standardized UWB channel model show how the number of antennas and that of prerake fingers affect the security performance.

Keywords: Multiple Antennas; Physical Layer; Prerake; Ultrawideband

1 Introduction

The broadcast nature of wireless channels necessitates securing the message transmission over such medium. While this need can be satisfied by using some kind of powerful encryption algorithms, low-power wireless systems such as radio frequency identification (RFID) systems may not even have enough power and resources to operate them [1,2,7,22,23]. Recent research on communication theory indicates that characteristics of ultrawideband (UWB) signals can be exploited to complement the levels of cryptographic security of wireless systems [5,11]. Specifically, the extremely large bandwidth of UWB signals makes their transmissions more robust to interference than narrow band transmissions. Moreover, since the transmit power of UWB devices is limited by relevant regulatory authorities such as the Federal Communications Commission (FCC) in the USA and the European Commission (EC) in Europe [9], these low-power devices are rather difficult to eavesdrop. UWB signaling such as impulse radio (IR) [24] can also be deliberately designed to achieve some level of encryption at the physical layer.

In the above design, a time-hopping sequence is adopted as a secret parameter for the UWB communication link [5,11]. That is, only a legitimate receiver who knows this sequence can successfully decode the overall message. In evaluating the physical-layer security performance of IR-UWB systems in [5,11], it is assumed that the transmitter, legitimate receiver, and adversary (*i.e.*, eavesdropper) are equipped with a single antenna. On the other hand, it is well known that the use of multiple antennas is capable of achieving spatial diversity. Many works such as [15, 21, 25, 27] have then focused on this deployment for UWB systems, resulting in significant performance improvement. To the best of our knowledge, however, the ability of multiple-antenna IR-UWB systems to support higher-layer cryptographic protocols has been investigated only in [26], where the authors presented a secure space-time coding scheme which uses channel state information (CSI) as the secret key in multiple-antenna links.[1] Unfortunately, an adversary still can employ the blind deconvolution method [6] to estimate its corresponding CSI, making it difficult for this scheme to attain the perfect communication secrecy.

In this paper, an alternative multiple-antenna IR-UWB system which can effectively provide the physical-layer security is proposed. Specifically, the transmitter employs multiple antennas to perform prerake filtering[2] with spatial transmit diversity, leading to temporal focusing (*i.e.*, the received signal is compressed in time domain) as well as spatial focusing (*i.e.*, the received signal is focused on the intended receiver, or more precisely, the legitimate one) [9]. Accordingly, the legitimate receiver who shares a common key with the transmitter requires only a simple matched filter to decode data. The security performance

[1] For the case of multiple-antenna narrow band systems, readers are referred to [10] and references therein.

[2] Another similar pre-filtering technique, called time reversal, has also been used in UWB communications [13, 27]. Nevertheless, this technique can be continuous-time processing based on physical waveform recording, and has a wider variety of applications such as electromagnetic imaging [14, 19] and underwater acoustic communications [4].

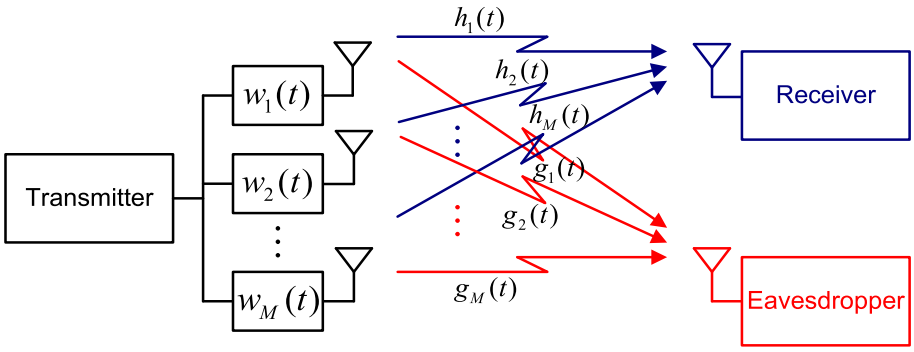

Figure 1: Multiple-antenna prerake UWB system

of the proposed system is also analytically evaluated in terms of the probability of the adversary correctly determining the key versus the decoding error probability of the legitimate receiver.

The rest of the paper is organized as follows. Section 2 describes the system model. In Section 3, the security performance of the multiple-antenna prerake UWB system is analyzed. Section 4 provides the numerical results, followed by the conclusion given in Section 5.

2 System Model

We consider a UWB system where the transmitter is equipped with M antennas, and the legitimate receiver as well as the eavesdropper are equipped with one antenna,[3] as shown in Figure 1. The M transmit antennas are spatially spaced in such a way that the transmitted signals undergo statistically independent channel fading.[4] In general, a UWB link channel can be modeled by the stochastic tapped-delay-line propagation model [9]. The channel impulse response (CIR) for a UWB transmission link from the transmitter to the legitimate receiver is thus described by

$$h_m(t) = \sum_{l=0}^{L_\mathrm{t}-1} \alpha_{m,l}\delta(t - lT_\mathrm{p}), \tag{1}$$

where $m \in \{1, 2, \ldots, M\}$ is the index of the transmit antenna, L_t is the number of multipath components, l is the path index, $\alpha_{m,l}$ is the energy-normalized path gain with $\sum_{l=0}^{L_\mathrm{t}-1} |\alpha_{m,l}|^2 = 1$, and T_p is the minimum multipath resolution. The minimum T_p is equal to the width of the unit-energy monocycle pulse $p(t)$, since any two paths whose relative delay is less than the pulse width are not resolvable. Similarly, the CIR for a UWB transmission link from the transmitter to the eavesdropper can be written as Equation (1) with $h_m(t)$ and $\alpha_{m,l}$ replaced by $g_m(t)$ and $\beta_{m,l}$, respectively.

As in [11], perfect timing and synchronization among the transmitter, legitimate receiver, and eavesdropper are assumed. Also, we suppose that a randomly generated b-bit secret key K is shared by the transmitter and the legitimate receiver, and it is divided into n parts, *i.e.*, $K = (\kappa_1, \kappa_2, \ldots, \kappa_n)$, to make use of the limited key bits.[5] The transmitter employs a time-hopping method and binary pulse amplitude modulation, and then uses each key part κ_j which consists of b/n bits, $j \in \{1, 2, \ldots, n\}$, to select a position index in $\{0, 1, \ldots, 2^{b/n} - 1\}$ that is shared by the pulses in the corresponding N_f/n frames (see Figure 2). Without loss of generality, we will consider an IR-UWB signal carrying the first binary data bit $b_0 \in \{-1, 1\}$ with equal probability in the first symbol period. To apply prerake filtering with spatial transmit diversity, the channel reciprocity is assumed to be satisfied,[6] and partial CSI of the links between the transmitter and legitimate receiver, *i.e.*, $\{\alpha_{m,l}\}_{m=1,l=0}^{M,L-1}$ with $L < L_\mathrm{t}$, is assumed to be known at the transmitter.[7] Therefore, a partial-prerake filter [20] with L taps (also called prerake fingers) can be used at the m-th antenna of the transmitter, and the transmitted signal is represented by

$$s_m(t) = \sqrt{\frac{E_\mathrm{s}}{N_\mathrm{f}}} \sum_{k=0}^{N_\mathrm{f}-1} b_0 z_m(t - kT_\mathrm{f} - c_{0,\lfloor \frac{nk}{N_\mathrm{f}} \rfloor} T_\mathrm{p}), \tag{2}$$

where E_s is the energy per symbol, N_f is the number of frames in one symbol period (denoted by $T_\mathrm{s} := N_\mathrm{f}T_\mathrm{f}$), T_f is the frame period, $\{c_{0,\lfloor \frac{nk}{N_\mathrm{f}} \rfloor}\}_{k=0}^{N_\mathrm{f}-1}$ is the time-hopping sequence, with $\lfloor \cdot \rfloor$ denoting the integer floor, and $z_m(t)$ is formed by passing the UWB pulse $p(t)$ through the

[3] The use of multiple antennas at the legitimate receiver and the eavesdropper is beyond the scope of this work and will be considered in our future work.

[4] In practice, such antenna spacing is expected to be on the order of a few ten centimeters [3].

[5] For simplicity, b is assumed to be divisible by n.

[6] The experimental results in [18] show that the reciprocal theorem is indeed valid for a UWB multipath environment.

[7] The reason behind the partial CSI consideration is as follows. In typical indoor UWB environments, the number of multipath components can be on the order of from several tens to a hundred more [16]. From a practical point of view, only a subset of the multipath components can be exploited at the transmitter or receiver side.

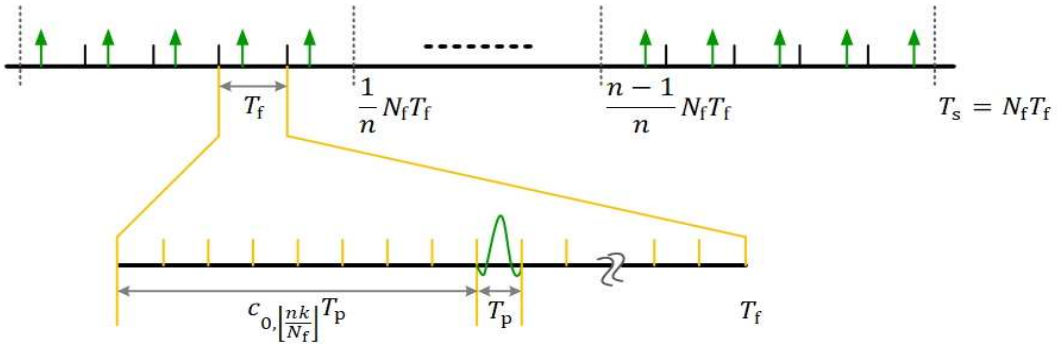

Figure 2: IR-UWB signal with secure time-hopping

partial-prerake filter $w_m(t)$. Mathematically speaking,

$$z_m(t) = w_m(t) * p(t) = \frac{1}{\sqrt{M\sum_{l=0}^{L-1}|\alpha_{m,l}|^2}} \sum_{l=0}^{L-1} \alpha^*_{m,L-1-l} p(t - lT_p), \quad (3)$$

where $*$ and $(\cdot)^*$ denote the convolution and complex conjugate, respectively, and the normalization factor $\sqrt{M\sum_{l=0}^{L-1}|\alpha_{m,l}|^2}$ is introduced in order to keep the total power transmitted from the M antennas constant [12]. The purpose of such filtering is to produce a strong peak of the received per-frame signal at the legitimate receiver, and then a matched filter (*i.e.*, single correlator) can be used to receive this path.

3 Performance Analysis

In the following, we will derive the error probabilities of the legitimate receiver and eavesdropper for the above system.

3.1 Legitimate Receiver

The IR-UWB signal received at the legitimate receiver can be expressed as

$$r(t) = \sum_{m=1}^{M} h_m(t) * s_m(t) + u(t) = \sum_{m=1}^{M}\sum_{l=0}^{L_t-1} \alpha_{m,l} s_m(t - lT_p) + u(t), \quad (4)$$

where $u(t)$ is the additive white Gaussian noise (AWGN) with zero mean and double-sided power spectral density (PSD) $N_0/2$. Based on Equations (2)-(4), it can be shown that the received signal $r(t)$ includes N_f strong paths (corresponding to N_f frames), and the delay of each relative to the first arrival path is $(L-1)T_p$. To perform matched filtering to these peaks, the legitimate receiver who knows the secrete key K (or more specifically, the time-hopping sequence $\{c_{0,\lfloor \frac{nk}{N_f} \rfloor}\}_{k=0}^{N_f-1}$) generates the template signal $v(t) = \frac{1}{\sqrt{N_f}}\sum_{k=0}^{N_f-1} p(t - kT_f - c_{0,\lfloor \frac{nk}{N_f} \rfloor}T_p)$. Thus, the decision variable for b_0 is given by

$$y = \mathrm{Re}\Bigg(\frac{1}{\sqrt{N_f}}\sum_{k=0}^{N_f-1}\Bigg[\int_{kT_f+c_{0,\lfloor \frac{nk}{N_f} \rfloor}T_p+(L-1)T_p}^{(k+1)T_f+c_{0,\lfloor \frac{nk}{N_f} \rfloor}T_p+(L-1)T_p} r(t) \times p(t - kT_f - c_{0,\lfloor \frac{nk}{N_f} \rfloor}T_p - (L-1)T_p)\,\mathrm{d}t\Bigg]\Bigg),$$

where $\mathrm{Re}(\cdot)$ denotes the real part. Following the same procedure as in [8], the bit error probability of the legitimate receiver conditioned on $\{\alpha_{m,l}\}_{m=1,l=0}^{M,L-1}$ is obtained as

$$P_b = Q\left(\sqrt{\frac{2E_s}{MN_0}}\sum_{m=1}^{M}\sqrt{\sum_{l=0}^{L-1}|\alpha_{m,l}|^2}\right) \quad (5)$$

where $Q(\cdot)$ denotes the Gaussian Q-function.

3.2 Eavesdropper

The IR-UWB signal received at the eavesdropper can be expressed as

$$\tilde{r}(t) = \sum_{m=1}^{M} g_m(t) * s_m(t) + \tilde{u}(t) = \sum_{m=1}^{M}\sum_{l=0}^{L_t-1} \beta_{m,l} s_m(t - lT_p) + \tilde{u}(t), \quad (6)$$

where $\tilde{u}(t)$ is the zero-mean AWGN with the same PSD as $u(t)$. In general, the eavesdropper is not likely to be very close to the legitimate receiver and then the received signal $\tilde{r}(t)$ in Equation (6) tends to be almost immersed in the background noise (see, *e.g.*, Figure 8 in [27], for an illustration). As a result, it is very difficult for the eavesdropper to find the data pulses without knowledge of their locations.

To establish a lower bound on the security performance, we focus on the worse-case scenario where the eavesdropper knows the transmitted data bit [11] in the sequel. Let us consider the first N_f/n frames, where data

pulses are located at the identical time slot in each frame. To use the matched filtering technique (similarly to the legitimate receiver), the eavesdropper generates the template signal $\tilde{v}_i(t) = \frac{b_0}{\sqrt{N_\mathrm{f}}} \sum_{k=0}^{N_\mathrm{f}/n-1} p(t - kT_\mathrm{f} - iT_\mathrm{p})$ when the data pulse is in the i-th time slot, $i \in \{0, 1, \ldots, 2^{b/n} - 1\}$. The decision statistic for the first N_f/n frames is therefore given by

$$\tilde{y}_i = \mathrm{Re}\Bigg(\frac{b_0}{\sqrt{N_\mathrm{f}}} \sum_{k=0}^{N_\mathrm{f}/n-1} \Bigg[\int_{kT_\mathrm{f}+iT_\mathrm{p}+(L-1)T_\mathrm{p}}^{(k+1)T_\mathrm{f}+iT_\mathrm{p}+(L-1)T_\mathrm{p}} \tilde{r}(t) \times p(t - kT_\mathrm{f} - iT_\mathrm{p} - (L-1)T_\mathrm{p})\, \mathrm{d}t \Bigg] \Bigg).$$

Note in Figure 2 that there are many slots in each frame due to the extreme bandwidth expansion, but only one of them contains a data pulse. Hence, the eavesdropper inevitably has to deploy the template at various delays, and then picks the output with the largest value. Following the approach outlined in [9, Chapter 6], it is straightforward to show that[8]

$$\tilde{y}_i \sim \mathcal{N}(\mu_i, \sigma^2),$$

where

$$\mu_i = \begin{cases} \mathrm{Re}\left(\frac{E_\mathrm{s}}{n} \sum_{m=1}^{M} \frac{\sum_{l=0}^{L+i-c_{0,0}-1} \alpha_{m,l-i+c_{0,0}}^{*} \beta_{m,l}}{\sqrt{M \sum_{l=0}^{L-1} |\alpha_{m,l}|^2}} \right), \\ \qquad (c_{0,0} - L + 1)\, U[c_{0,0} - L + 1] \le i \le c_{0,0} \\ \mathrm{Re}\left(\frac{E_\mathrm{s}}{n} \sum_{m=1}^{M} \frac{\sum_{l=i-c_{0,0}}^{L+i-c_{0,0}-1} \alpha_{m,l-i+c_{0,0}}^{*} \beta_{m,l}}{\sqrt{M \sum_{l=0}^{L-1} |\alpha_{m,l}|^2}} \right), \\ \qquad c_{0,0} + 1 \le i \le L_\mathrm{t} - L + c_{0,0} \\ \mathrm{Re}\left(\frac{E_\mathrm{s}}{n} \sum_{m=1}^{M} \frac{\sum_{l=i-c_{0,0}}^{L_\mathrm{t}-1} \alpha_{m,l-i+c_{0,0}}^{*} \beta_{m,l}}{\sqrt{M \sum_{l=0}^{L-1} |\alpha_{m,l}|^2}} \right), \\ \qquad L_\mathrm{t} - L + c_{0,0} + 1 \le i \le L_\mathrm{t} + c_{0,0} - 1 \\ 0, \ \text{otherwise}, \end{cases} \tag{7}$$

and

$$\sigma^2 = \frac{N_0}{2}. \tag{8}$$

In Equation (7), $c_{0,0}$ is the actual time-hopping subsequence for the first N_f/n frames, and $U[\,\cdot\,]$ denotes the discrete-time unit step function. Applying the result of optimal detection for orthogonal signaling in [17, Chapter 4], the probability of finding the correct pulse position in the first N_f/n frames conditioned on $\{\alpha_{m,l}^{*}\}_{m=1,l=0}^{M,L-1}$ and $\{\beta_{m,l}\}_{m=1,l=0}^{M,L_\mathrm{t}-1}$ is obtained as

$$\Pr\{\tilde{y}_i < \tilde{y}_{c_{0,0}}, \forall i \ne c_{0,0}\} = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \left[\prod_{i=0, i\ne c_{0,0}}^{2^{b/n}-1} \left(1 - Q\left(\frac{x - \mu_i}{\sigma} \right) \right) \right] \times \exp\left(-\frac{(x - \mu_{c_{0,0}})^2}{2\sigma^2} \right) \mathrm{d}x.$$

[8] To obtain this closed-form expression, we assume that $T_\mathrm{f} > (2L_\mathrm{t} + 2^{b/n} - 1)T_\mathrm{p}$.

Because the time-hopping subsequence for each group of N_f/n frames is independently assigned by the corresponding key part, the conditional probability of error for finding the entire key at the eavesdropper is given by

$$P_\mathrm{e} = 1 - \left(\Pr\{\tilde{y}_i < \tilde{y}_{c_{0,0}}, \forall i \ne c_{0,0}\} \right)^n. \tag{9}$$

4 Numerical Results

A description of the security performance of the proposed system can be obtained by plotting the average probability of the eavesdropper correctly determining the key (*i.e.*, $1 - \bar{P}_\mathrm{e}$) versus the average bit error probability of the legitimate receiver (*i.e.*, $\bar{P}_\mathrm{b}$) on a log-log scale, as shown in Figures 3-5. For these plots, the parameters are set as follows: $b = 30$, $n = 5$, $N_\mathrm{f} = 25$, $T_\mathrm{f} = 400$ ns, and $T_\mathrm{p} = 125$ ps. Furthermore, the received signal-to-noise (SNR) ratio is assumed to be the same at the legitimate receiver and the eavesdropper, while $\bar{P}_\mathrm{b}$ and $\bar{P}_\mathrm{e}$ are obtained, respectively, by averaging Equations (5) and (9) over 10,000 channel realizations generated from one of the IEEE 802.15.4a channel models, namely CM3 for an office line-of-sight environment [16]. The label "ideal" refers to the case in which $L = L_\mathrm{t}$.

Figure 3 compares the security performance of our prerake UWB system and the rake UWB (or more specifically, baseline) system proposed in [11] when both systems use a single transmit antenna ($M = 1$). The results in this figure show that, with the same number of fingers (L), the former system outperforms the latter one. This may be explained, for example, by considering the mean (μ_i) and variance (σ^2) of $\tilde{y}_i$ for the two systems. From Equations (7) and (8), we have $\mu_{c_{0,0}} = \mathrm{Re}\left(\frac{E_\mathrm{s}}{n} \frac{\sum_{l=0}^{L-1} \alpha_l^{*} \beta_l}{\sqrt{\sum_{l=0}^{L-1} |\alpha_l|^2}} \right)$ and $\sigma^2 = \frac{N_0}{2}$ for the prerake UWB system with $M = 1$,[9] while its rake counterpart (see [11, Section IV-B]) yields $\mu_{c_{0,0}} = \frac{E_\mathrm{s}}{n} \sum_{l=0}^{L-1} |\beta_l|^2$ and $\sigma^2 = \frac{N_0}{2} \sum_{l=0}^{L-1} |\beta_l|^2$. In our simulation trials, we find that the first mean $\mu_{c_{0,0}}$ tends to be less than the second one. Meanwhile, the first variance σ^2 is obviously larger than the second one. For these reasons, the prerake UWB system generally has a lower value of $\Pr\{\tilde{y}_i < \tilde{y}_{c_{0,0}}, \forall i \ne c_{0,0}\}$ and thus a higher probability of error P_e.

Figures 4 and 5 show the security performance of the prerake UWB system with two transmit antennas ($M = 2$) and that with four transmit antennas ($M = 4$), respectively. As seen in these figures, the system performance improves when the number of antennas or the number of fingers is increased. This improvement results from the temporal and spatial focusing described in Section 1. In addition, by varying those two numbers while keeping their product constant, increasing the number of antennas is found to be more beneficial to the system performance than increasing the number of fingers. For example, when the average bit error probability of the legitimate receiver for $M = 1$ and $L = 20$ and that for

[9] For notational simplicity, we omit the antenna index m.

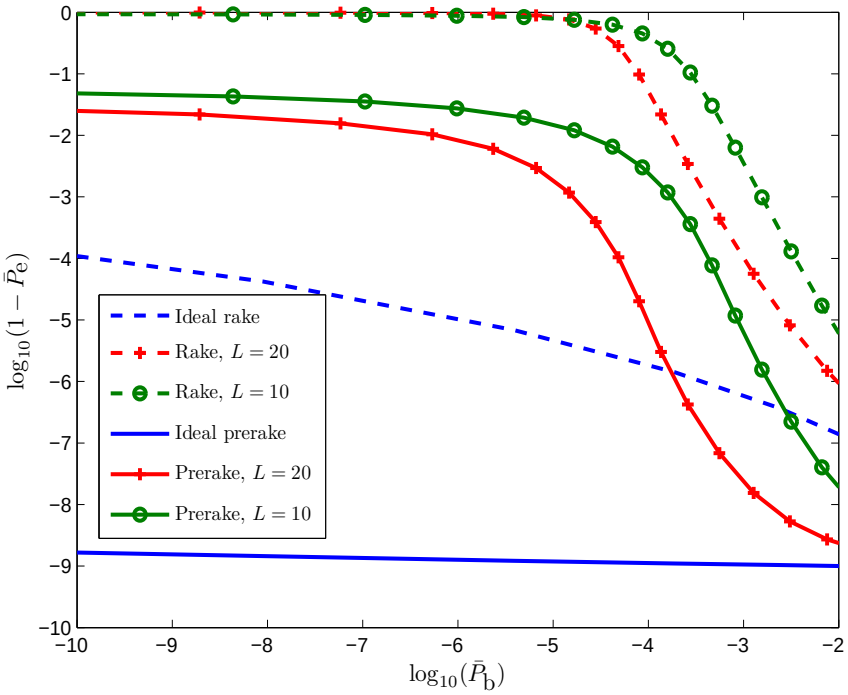

Figure 3: Performance comparison of rake and prerake UWB systems ($M = 1$)

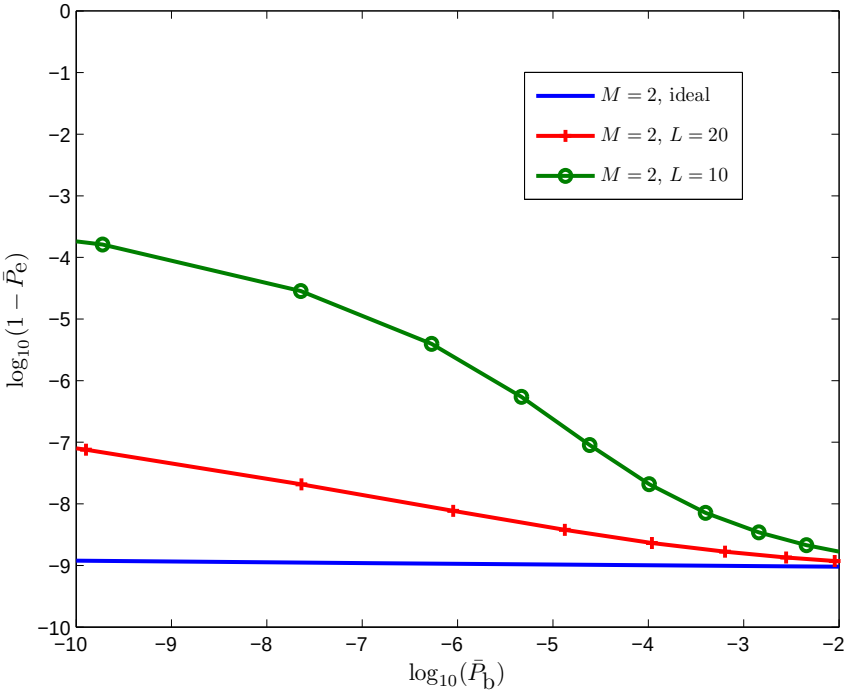

Figure 4: Security performance for different number of prerake fingers ($M = 2$)

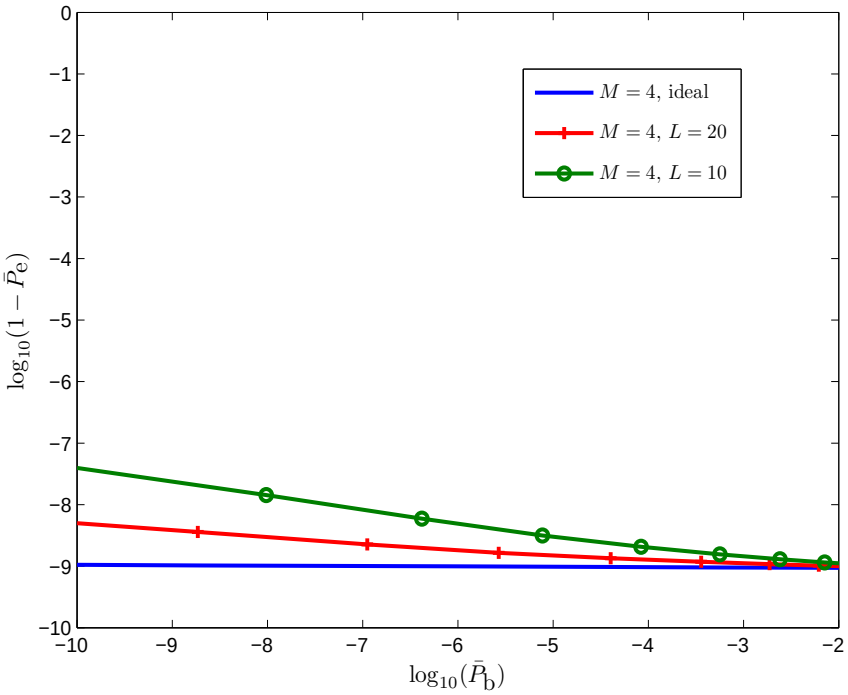

Figure 5: Security performance for different number of prerake fingers ($M = 4$)

$M = 2$ and $L = 10$ are 10^{-4}, the average probabilities of the eavesdroppers correctly determining the key are approximately 10^{-5} and 10^{-8}, respectively. This is due to the fact that the power delay profile of the considered UWB channel model is exponentially decaying [16].

5 Conclusion

We have presented a multiple-antenna prerake UWB system which enables the key-and-location-based security and can satisfactorily thwart the adversary in eavesdropping. The bit error probability of the legitimate receiver and the probability of the adversary finding the correct positions for data pulses have been derived. The performance results have suggested that deploying multiple antennas can save the numbers of prerake fingers, which is required to achieve a high physical-layer security. As our results do not take account of spatial correlation between the transmitter-to-legitimate-receiver and transmitter-to-adversary links, the effect of this correlation on the security performance will be examined in future work.

References

[1] Y. C. Chen, W. L. Wang, and M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection," in *Proceedings of The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[2] P. Cui, "An improved ownership transfer and mutual authentication for lightweight RFID protocols," *International Journal of Network Security*, vol. 18, no. 6, pp. 1173–1179, 2016.

[3] R. D'Errico, A. Sibille, A. Giorgetti, and M. Chiani, "Antenna diversity in UWB indoor channel," in *Proceedings of IEEE International Conference on Ultra-Wideband*, pp. 13–16, Sep. 2008.

[4] G. F. Edelmann, H. C. Song, S. Kim, W. S. Hodgkiss, W. A. Kuperman, and T. Akal, "Underwater acoustic communications using time reversal," *IEEE Journal of Oceanic Engineering*, vol. 30, no. 4, pp. 852–864, 2005.

[5] D. S. Ha and P. R. Schaumont, "Replacing cryptography with ultra wideband (UWB) modulation in secure RFID," in *Proceedings of The First IEEE Conference on Radio Frequency Identification*, pp. 23–29, Mar. 2007.

[6] Y. Hua, S. An, and Y. Xiang, "Blind identification of FIR, MIMO channels by decorrelating subchannels," *IEEE Transactions on Signal Processing*, vol. 51, no. 5, pp. 1143–1155, 2003.

[7] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols," in *Proceedings of The 25th Annual International Cryptology Conference*, pp. 293–308, Aug. 2005.

[8] M. Jun and T. Oh, "Performance of pre-rake combining time hopping UWB system," *IEEE Transactions*

on Consumer Electronics, vol. 50, no. 4, pp. 1033–1037, 2004.

[9] T. Kaiser and F. Zheng, *Ultra Wideband Systems with MIMO*, 2010. ISBN:9780470740019.

[10] J. Kitchen, *On MIMO Wireless Eavesdrop Information Rates*, 2011. (`http://hdl.handle.net/11343/36890`)

[11] M. Ko and D. L. Goeckel, "Wireless physical-layer security performance of UWB systems," in *Proceedings of IEEE Military Communications Conference*, pp. 2143–2148, Nov. 2010.

[12] P. Kyritsi, G. Papanicolaou, P. Eggers, and A. Oprea, "MISO time reversal and delay-spread compression for FWA channels at 5 GHz," *IEEE Transactions on Antennas and Propagation*, vol. 3, no. 11, pp. 96–99, 2004.

[13] X. Liu, B. Z. Wang, S. Xiao, and J. Deng, "Performance of impulse radio UWB communications based on time reversal technique," *Progress in Electromagnetics Research*, vol. 79, pp. 401–413, 2008.

[14] N. Maaref, P. Millot, X. Ferrieres, C. Pichot, and O. Picon, "Electromagnetic imaging method based on time reversal processing applied to through-the-wall target localization," *Progress in Electromagnetics Research M*, vol. 1, pp. 59–67, 2008.

[15] K. Maichalernnukul, T. Kaiser, and F. Zheng, "On the performance of coherent and noncoherent UWB detection systems using a relay with multiple antennas," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3407–3414, 2009.

[16] A. F. Molisch, D. Cassioli, C. C. Chong, S. Emami, A. Fort, B. Kannan, J. Karedal, J. Kunisch, H. G. Schantz, K. Siwiak, and M. Z. Win, "A comprehensive standardized model for ultrawideband propagation channels," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 11, pp. 3151–3166, 2006.

[17] J. G. Proakis and M. Salehi, *Digital Communications*, 2008. (`https://www.amazon.com/Digital-Communications-5th-John-Proakis/dp/0072957166`)

[18] R. C. Qiu, C. Zhou, N. Guo, and J. Q. Zhang, "Time reversal with MISO for ultrawideband communications: Experimental results," *IEEE Antennas and Wireless Propagation Letters*, vol. 5, no. 1, pp. 269–273, 2006.

[19] A. B. Ruffin, J. Van Rudd, J. Decker, L. Sanchez-Palencia, L. Le Hors, J. F. Whitaker, and T. B. Norris, "Time reversal terahertz imaging," *IEEE Journal of Quantum Electronics*, vol. 38, no. 8, pp. 1110–1119, 2002.

[20] K. Usuda, H. Zhang, and M. Nakagawa, "Pre-rake performance for pulse based UWB system in a standardized UWB short-range channel," in *Proceedings of IEEE Wireless Communications and Networking Conference*, pp. 920–925, Mar. 2004.

[21] L. C. Wang, W. C. Liu, and K. J. Shieh, "On the performance of using multiple transmit and receive antennas in pulse-based ultrawideband systems," *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 2738–2750, 2005.

[22] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "A mutual authentication protocol for RFID," *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[23] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[24] M. Z. Win and R. A. Scholtz, "Impulse radio: How it works," *IEEE Communications Letters*, vol. 2, no. 2, pp. 36–38, 1998.

[25] L. Yang and G. B. Giannakis, "Analog space-time coding for multiantenna ultra-wideband transmissions," *IEEE Transactions on Communications*, vol. 52, no. 3, pp. 507–517, 2004.

[26] Y. Zhang and H. Dai, "A real orthogonal space-time coded UWB scheme for wireless secure communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–8, 2009.

[27] C. Zhou, N. Guo, and R. C. Qiu, "Time reversed ultra-wideband (UWB) multiple-input multiple-output (MIMO) based on measured spatial channels," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 2884–2898, 2009.

Biography

Tanit Somleewong received the B.E. degree from Mahanakorn University of Technology, Thailand, in 1997 and the M.S. degree from Walailak University, Thailand, in 2004. He is currently working toward the Ph.D. degree with College of Information and Communication Technology, Rangsit University, Thailand.

Kiattisak Maichalernnukul received the Dr.-Ing. degree (summa cum laude) in electrical engineering from University of Hannover, Germany, in 2010. From 2005 to 2006, he was a Research Assistant with the National Electronics and Computer Technology Center, Thailand. From 2007 to 2011, he was a Scientific Assistant with the Institute of Communications Technology, University of Hannover. Since July 2011, he has been a Lecturer with Rangsit University, Thailand. His research interests are in the areas of communication theory and signal processing for wireless communications. He received an Information Technology Society (ITG) Dissertation Prize from the German Association for Electrical, Electronic, and Information Technologies (VDE) in 2011 and a Young Scientist Award from the URSI Asia-Pacific Radio Science Conference (AP-RASC) in 2013.