Physical Layer Security Using Multi-band Transmission Considering Channel Selection for Cognitive Radio Networks

Akinari Ida† Takeo Fujii†

†Advanced Wireless Communication research Center (AWCC), The University of Electro-Communications
1-5-1, Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan
{a-ida, fujii}@awcc.uec.ac.jp

***Abstract*— In this paper, we consider a secrecy transmission scheme based on physical layer, employing multi-band transmitters with dynamic power allocations and channel selections under the circumstance of spectrum sharing cognitive radio networks. Here, we apply a physical layer security utilizing multi-band transmitter for distributing each confidential message of each receiver over multiple frequency channels and for decreasing leakage. Moreover, we aim to improve the secrecy capacity by using a channel selection method based on the channel condition of each user and primary usage. By using computer simulations, we could verify that the proposed method improves the performance in terms of secrecy capacity against eavesdropping compared with methods using single-band transmission under primary user coexisting environment.**

I. INTRODUCTION

In recent years, wireless communications such as wireless local area networks (WLANs) and cellular networks have become popular worldwide. However, wireless communications is facing shortage of frequency resource. To solve this issue, cognitive radio technologies as a radical solution have attracted attention [1]. In cognitive radio, the secondary user (SU) can change the communication parameters according to the surrounding wireless environment and access a vacant spectrum called White Space (WS), which is the temporally or spatially unutilized spectrum band allocated to the primary user (PU). In related studies, a variety of methods has been considered to increase the capacity or throughput for SU [2]. By contract, SU has the issue of the information leaking because the wireless channels are shared with multiple systems and exposed to the area where the radio waves are propagated. Generally, at the transmitter side, a cryptographic security, which provides intractability achieved by solving factorization into prime factors [3] and a security with secret key [4] have been utilized. However, the secure level is degraded by increasing competency of eavesdroppers.

In addition, security provisions in the physical (PHY) layer have been widely studied because those are not affected by eavesdropper's computational ability, and have possibility of keeping security in wireless domain. In early works for PHY layer security [5]-[7], Wyner [5] introduced the security problem in the wiretap channel, and it is extended to the case of the Gaussian channel [4]. Then, Csiszar and Korner considered security problems in broadcast channels [7]. Until now, many works for PHY layer security in wireless communication have been studied, and mainly focus on having the transmitted message independent from the eavesdropper's receipt of a message to achieve perfect secrecy. In [5]-[7], it is shown that a positive secrecy capacity can be obtained if legitimate transmission rate is larger than the channel capacity for eavesdropper. At that time, secrecy capacity C_s is defined as the difference between the capacity for legitimate link and for illegal link. Recently, it has been discussed that the secrecy capacity C_s has to be modified to take account PHY layer parameters such as modulation, coding, transmitting control, etc. In particular, in secrecy transmission, there are few schemes for avoiding a channel being wiretapped owing to the frequency-dispersal. In addition, there are schemes which apply chaos modulation to the MIMO antenna multiplexing [8], and redundant information to the message-bearing signal utilized for wireless sensor networks [9]. However, these methods are information dispersal for a single frequency channel when giving a message redundancy or randomness. Accordingly, in the case that the detection ability of eavesdropper is high, secure communication cannot be promised as similar to cryptographic security and security for secret key.

Therefore, in this paper, in order to enhance secrecy capacity C_s, we focus on secret sharing transmission [10] over frequency, and propose multi-band transmission, where the transmitter uses multiple frequency channels to distribute different confidential messages to intended receiver. When an eavesdropper wiretaps arbitrary frequency channel, we can avoid the attack by dispersing the messages on the multiple frequency channels. Here, multiband transmission is utilized in cognitive radio networks, which have been considered to improve the efficiency of frequency usage and system capacity. The proposed multi-band transmission is used for distributing a message over the multiple frequency channels and dealing each channels to improve C_s. Furthermore, we bring difference between the channel capacity C_e for illegal link and the channel capacity C for legitimate link to apply channel selection with protecting the PU based on the channel condition of each user and status of utilization for PU. This application is designed on the idea of [11], i.e., the C_s can be improved if the legitimate link channel is better than the illegal link channel. In the channel selection, if the transmitter SU chooses the channel used by PU, it needs to control transmitted power to allowed power level at PU. At the same

978-616-361-823-8

time, SU and eavesdropper receive interference signal from PU.

The rest of this paper is organized as follows. In Section II, we introduce the system configuration. Next, the proposed multi-band transmission for channel selection is presented in Section III. Computer simulation results for verifying the performance of the proposed method are shown in Section IV. Finally, we provide some concluding remarks in Section V.

II. System Model

In this paper, we assume that a legitimate transmitter SU_{tx} communicates with its corresponding receiver SU_{rx} in the presence of eavesdropper and PU. Figure 1 shows a system model assumed in this paper. In this section, we explain a system model, channel model, and protection strategy for PU utilizing in this paper by using equations.

A. Secrecy Capacity including a signal for PU

In order to calculate the received power (denoted as P_r in dBm) for the 1-frequency channel-case, the following propagation loss model can be considered

$$P_r = P_t + 10\log_{10}\left(\frac{\lambda}{4\pi d_0}\right)^2 + 10\gamma\log_{10}\frac{d_0}{d}, \quad (1)$$

where the gain of each antenna is defined as 0 dBi. p_t, λ, d_0, γ and d are transmitted power in dBm, wave length of a signal, reference distance, pass loss gain, and distance between the transmitter and the receiver, respectively. Using equation (1), we calculate p_r against p_t and signal to interference and noise ratio (SINR) between a transmitter (SU_{tx}) and a receiver (SU_{rx}). Then, $SINR$ of SU_{rx} and Eve are given by equations (2) and (3),

$$SINR_{\text{tx\_rx}} = \frac{\|h_{\text{tx\_rx}}\|^2 P_{\text{r\_SU}}}{\|h_{\text{pu\_rx}}\|^2 P_{\text{PU\_SU}} + N_0 B}, \quad (2)$$

$$SINR_{\text{tx\_eve}} = \frac{\|h_{\text{tx\_eve}}\|^2 P_{\text{r\_EVE}}}{\|h_{\text{pu\_eve}}\|^2 P_{\text{PU\_EVE}} + N_0 B}, \quad (3)$$

where, $h_{\text{tx\_rx}}$, $h_{\text{tx\_eve}}$, $h_{\text{pu\_rx}}$, $h_{\text{pu\_eve}}$ are channel gain for SU_{tx}- SU_{rx}, SU_{tx}- Eve, PU- SU_{rx} and PU- Eve link respectively, N_0 is noise power, and B is bandwidth. Using equation (2), channel capacity $C_{\text{tx\_rx}}$ can be described as,

$$C_{\text{tx\_rx}} = B\log_2(1 + SINR_{\text{tx\_rx}}), \quad (4)$$

In addition, the channel capacity $C_{\text{tx\_eve}}$ between SU_{tx} and an eavesdropper can be written as,

$$C_{\text{tx\_eve}} = B\log_2(1 + SINR_{\text{tx\_eve}}), \quad (5)$$

where, $SINR_{\text{tx\_eve}}$ means $SINR$ for eavesdropper. Hereafter, we focus on secrecy capacity of the multi-band and the single-band transmission. We assume that the transmitted message, W, is independent from the message received by the eavesdropper, Z, i.e., $I(W;Z) = 0$, meaning that perfect secrecy is achieved. Accordingly, the legitimate transmission rate R satisfies $C_e < R < C$, where C and C_e are the channel capacity for the transmitter and for an eavesdropper, respectively.

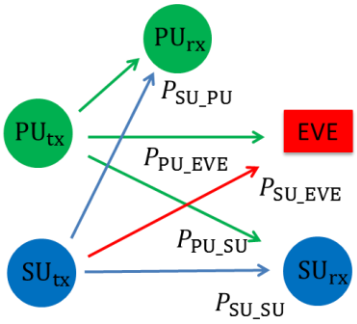

Fig.1 System model.

At the same time, from equations (4) and (5), we can obtain secrecy capacity C_s in the 1-channel communication [11] as

$$C_s = C_{\text{tx\_rx}} - C_{\text{tx\_eve}}, \quad (6)$$

where min C_s is 0.

B. Channel Model and Protection of PU

We assume that SU_{tx} senses channel $i(\in L, bandwth = B[MHz])$ perfectly as shown in Figure 2. If SU_{tx} selects PU channel, SU_{tx} needs to control the transmitted power P_t to protect the PU. When SU_{tx} can use maximum power $P_{\max}$, P_t is expressed as

$$P_{\text{t}} \le \Gamma \quad \text{if channel is PU}, \quad (7)$$

$$P_{\text{t}} = P_{\max} \quad \text{if channel is WS}, \quad (8)$$

where Γ is the interference power which can be allowed to PU. Then, if the allowed interference powerΓ at PU is given, P_{t} can be calculated by equation (1).

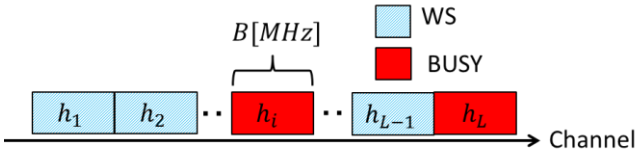

Fig.2 Channel statement.

III. Proposed Method

In this section, we present a proposed multi-band transmission and channel selection based on the channel condition of each channel and PU usage. First, we present a multi-band transmission and lead secrecy capacity from the basis of prior chapter II. Next, we introduce the channel selection criterion.

A. Multi-band Transmission

In the proposed multi-band transmission, the transmitter selects n-frequency channels from L-frequency channels, and sends different messages dispersed on n-channels in parallel. In case of common 1-channel transmission, i.e., single-band transmission, all information can be eavesdropped if eavesdropper catches the channel in use. In contrast, multi-band transmission can decrease the amount of eavesdropping owing to the frequency-dispersal effect. Frequency channels

chosen by the multi-band transmitter are composed of multiple sub-channels given by dividing one frequency band B into n-channels $\frac{B}{n}$. At the same time, the frequency channel chosen by single-band transmission is composed of 1-channel which is not divided. Figure 3 shows an example of signal propagation for the single-band transmission and the multi-band transmission when eavesdropper wiretaps j-channel

Compared to single-band transmission, in the multi-band transmission, transmitter uses orthogonal frequency channels to send different confidential messages to the intended receiver. We therefore can determine C_{s_Multi} by

$$C_{\text{s\_Mulit}} = \sum_{i=1}^{n} (C_{s\_i})^{+}, \tag{9}$$

where, $(\cdot)^{+} = \max\{0,\cdot\}$ and C_{s_i} is secrecy capacity for i-sub channel. When the eavesdropper wiretaps sub-channels $\{j \mid 0 \le j \le n\}$, considering sub-channel j, C_{s_i} is described into two types as follows:

$$C_{\text{s\_}i} = \frac{B}{n} C_{\text{tx\_rx\_}i} - \frac{1}{n} C_{\text{tx\_eve\_}i} \quad (i = j), \tag{10}$$

$$C_{\text{s\_}i} = \frac{B}{n} C_{\text{tx\_rx\_}i} \quad (i \neq j), \tag{11}$$

where $C_{\text{tx\_rx\_}i}$ and $C_{\text{tx\_eve\_}i}$ are the channel capacity of sub-channel i allocated to legitimate link and illegality link, respectively. That is, (10) and (11) are the channel capacities when sub-channel i is wiretapped and not wiretapped, respectively. Besides, the secrecy capacity $C_{\text{s\_Single}}$ in the single-band transmission, can be determined by (12), whereas that of the multi-band transmission, C_{s_i}, can be determined by (13) and (14) for both cases that sub-channel i is wiretapped and not wiretapped.

$$C_{\text{s\_Single}} = (C_{s\_i})^{+}. \tag{12}$$

$$C_{\text{s\_}i} = C_{\text{tx\_rx}} - C_{\text{tx\_eve}} \quad (i = j). \tag{13}$$

$$C_{\text{s\_}i} = C_{\text{tx\_rx}} \quad (i \neq j). \tag{14}$$

B. Channel Selection

For the channel selection, we choose the n best sub channels which enhance $SINR$ in descending order from all the L sub channels as shown in Figure 4. The selection criterion for i sub-channel is given by equation (15),

$$\max_{\text{tx\_rx\_}i \in L} \frac{\|h_{\text{tx\_rx\_}i}\|^2 P_r}{\|h_{\text{pu\_rx\_}k}\|^2 P_{\text{PU\_SU}} + N_0 B}. \tag{15}$$

Since SU_{tx} selects a channel according to $\max_{i \le \in L} SINR_i$, if SINR is larger, the selected channel is shared with PU channel. At that time, the transmitted power P_{t} is controlled to satisfy equation (7). If the channel does not have PU signal, $\|h_{\text{pu\_rx\_}k}\|^2 P_{\text{PU\_SU}} = 0$. From selection criterion (15), we can find 3 components that influence to $SINR_i$ and C_{s} as follows.

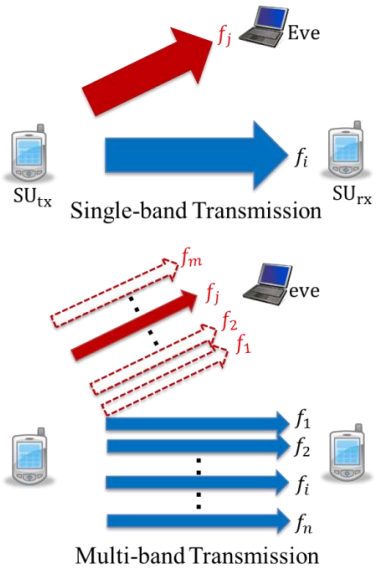

Fig.3 Single-band and Multi-band Transmission.

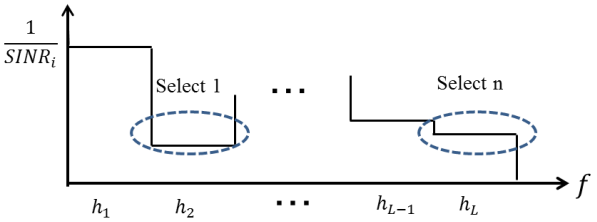

Fig.4 Channel Selection.

(A) If the channel condition of $h_{\text{tx\_rx\_}i}$ is greater than $h_{\text{tx\_eve}}$, C_s can be improved.

(B) If PU channel with controlling transmitted power for keeping PU performance is selected, both $SINR_{\text{tx\_rx}}$ and $SINR_{\text{tx\_eve}}$ becomes lower.

(C) If PU channel is selected, $SINR_{\text{tx\_rx}}$ degrades if there is PU_{tx} around SU_{tx} nearer than Eve.

In the proposed channel selection, we adopt the value of $SINR_{\text{tx\_rx}}$ considering above 3 components.

IV. Simulation Result

In this section, we show the simulation results of the single-band transmission and the proposed method designed for sending different confidential message by using multi-band transmission with the channel selection. We assume that a transmitter and a receiver are located in $(0,0)$, $(50,0)$, respectively, and the distance between the transmitter and the eavesdropper varies from 0[m] to 150[m]. PU_{tx} and PU_{rx} are respectively located in a 100[m] radius from (0,0) randomly.

Among three channels, the single-band transmitter chooses one of the channels each of which comprises ten frequency bands of 5[GHz] bandwidth and then, sends the message over the channel. On the other hand, the multi-band transmitter uses all the three sub-channels divided one frequency bandwidth into 3-sub-channels in 5[GHz] as shown in Figure 5, and sends messages over the three sub-channels. The

channel usage of PU varies from 0[%] to 100[%], that is 0,-3..27,30[channels].

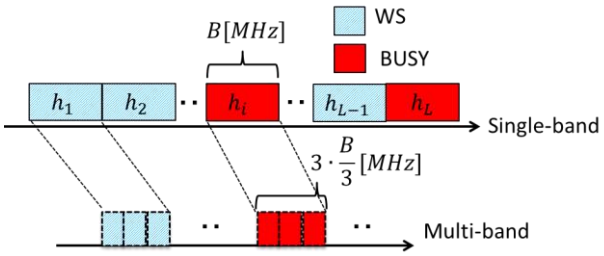

Fig.5 Dividing one channel into $n = 3$ channels.

Each transmitter does not utilize the information of eavesdropper. It needs to remark that SU_{tx} select a channel according to only $\max_{i \le \in L} SINR_i$, not the information of eavesdropper. Eavesdropper can wiretap the channel as many as that of each transmitter, and bandwidth of each transmitter.

In this paper, we assume two scenarios about eavesdropper's channel detection. One story is that eavesdropper wiretaps a channel with random. The other is that eavesdropper detects WS and wiretaps the WS channel. In each case, SU_{tx} utilizing the proposed channel selection which is based on $SINR$. In the case of random wiretap, $P_r(j)$ with diverse $j's$ are shown in Table 1, where $P_r(j)$ is the probability that j sub-channels are wiretapped. In the other case of WS wiretap, the probability of wiretapped at least 1 channel for multi-band transmission $P_r(j \ge 1)$ vs the channel usage of PU is shown in Figure 6. The channel usage of PU means the number of channels utilized by PU. We also take the case of random wiretap into Fig. 6. When the channel usage is 100[%], we deal the probability $P_r(j)$ as random wiretapped case. The simulation parameters in this paper are shown in Table 2. Then, we evaluate the secrecy capacity achieved by each transmission as shown in Fig.7 to Fig.9, where n and L are 3, 10, respectively.

From Table 1, we can find that the probability of wiretapped randomly for multi-band transmission is dividing into 3 channels in each. In contrast, from Fig. 6, the channel usage of PU increases, if an eavesdropper wiretaps the WS channel the probability $P_r(j)$ outperforms over the attack of random wiretap. When the channel usage of PU is 90[%], the probability $P_r(j)$ is larger by 0.36 points compared with random wiretap.

Figure 7 shows secrecy capacity obtained by each transmission utilizing the proposed channel selection, where j channels are wiretapped and the channel usage of PU is 50[%]. In Fig. 7, we can verify secrecy capacity value higher than 0 over eavesdropper anywhere with the exception of Multi-$P_r(3)$. When all the channels are not wiretapped, i.e., $P_r(0)$, the performance curve C_s is improved to C_{tx_rx} which is upper-bound of C_s for each transmission. In the multi-band transmission, the curve in wiretapped closest to the upper-bound is obtained when $P_r(1)$ =0.09. Moreover, compared with single-band transmission in wiretapped, the multi-band transmitter has higher secrecy capacity, especially eavesdropper located in more than 20[m] apart from the transmitter. Although single-band transmission cannot protect the security, multi-band transmission utilizing channel selection makes the area in 20[m] secure.

TABLE 1

P_m in each Transmissions (Random wiretap).

$P_r(m)$ \ m	0	1	2	3	
P_{Single}	0.9	0.1			Total=1
P_{Multi}	0.72	0.26	0.02	0.0003	Total=1

TABLE 2

Simulation Parameters.

Total transmitted power	10[dBm]
PU's transmitted power	10[dBm]
The number of channels utilized by PU	0〜30
Allowed interference power at PU	-90[dBm]
AWGN	-108[dBm/MHz]
Fading	Rayleigh
Avalable freqency band	5.18〜5.36[GHz]
Reference distance	10[m]
Pass loss index	3

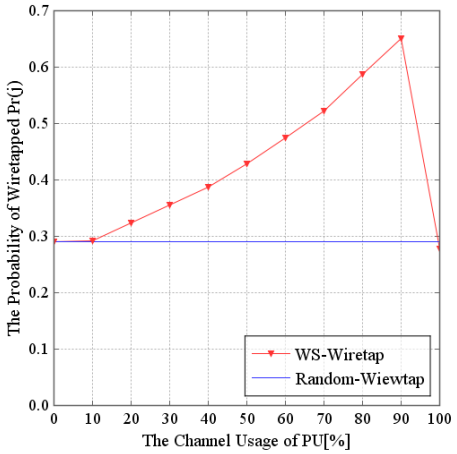

Fig.6 $P_r(j \ge 1)$ vs The channel usage of PU.

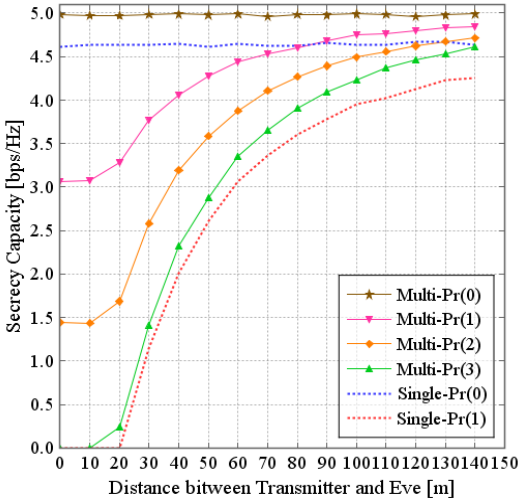

Fig.7 Multi vs Single-band by $P_r(j)$.

Figure 8 shows secrecy capacity performance using the proposed channel selection (SINR-based-CS) and the

compared channel selection (H-based-CS), which selects the channel based on only the channel condition h. Here, the probability $P_r(j)$ of H-based-CS follows Random wiretap in Fig.6 because of random channel generation. Then, from Fig.8 we confirm that although the probability $P_r(j)$ of SINR-based-CS is larger than that of H-based-CS in WS attacked by eavesdropper, SU can gain higher secrecy capacity rather than H-based-CS. This is because SINR-based-CS is influenced by the channel selection criterion affected by PU existence and selects the channel which enhances SINR.

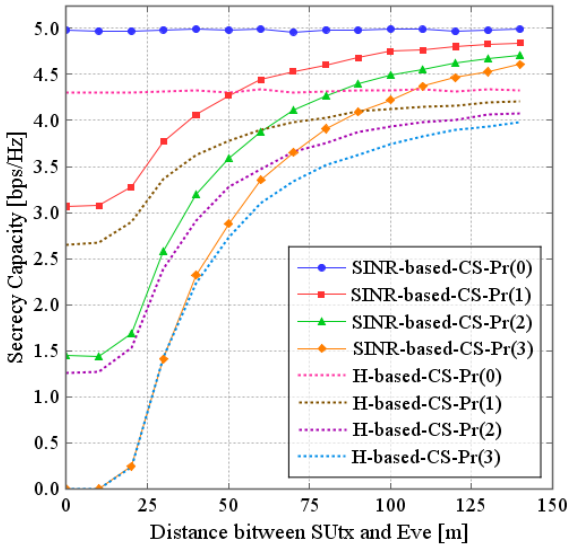

Fig.8 SINR-based vs H-based Channel Selection.

Figure 9 shows secrecy capacity curves used SINR-based-CS with eavesdropper in 70[m], 50[m] and 30[m] in $P_r(1)$, respectively. The channel usage of PU varies from 0 to 100[%]. In Fig.9, we can see that, when the eavesdropper is 70[m] far from the transmitter, it is 35[%] decreasing in terms of secrecy capacity from 0 to the maximum channel usage of PU. On the other hand, when the distance between SU_{tx} and Eve varies from 70[m] to 30[m], secrecy capacity degrades 15[%]. Then, we confirm that the channel usage of PU influences secrecy capacity larger than eavesdropper's location in the area $C_s > 0$.

V. Conclusion

In this paper, in order to enhance the secrecy capacity, we focused on the secret sharing transmission over frequency, and proposed a novel multi-band transmission, where the transmitter uses multiple frequency channels for distributing different confidential messages intended to a receiver. Furthermore, we considered the channel selection based on the channel condition of each user and the channel usage of PU in order to make difference between C_e and C. From the numerical simulation results, we confirmed that applying the proposed method improves the secrecy capacity even though the proposed scheme outperforms in P_m over the WS attacked by eavesdropper. In contrast, by applying the proposed channel selection, we could improve the secrecy capacity compared with the low wiretap probability method which selects the channel based on only the channel condition.

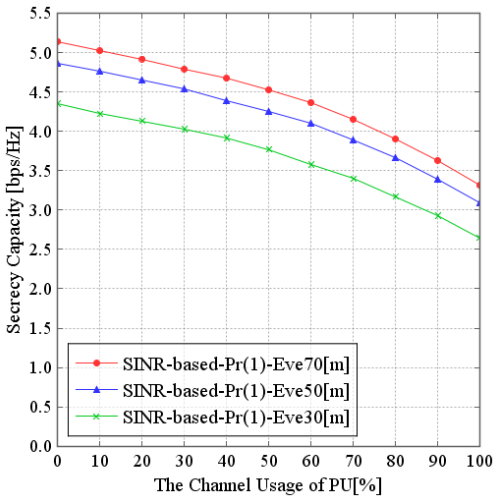

Fig.9 Cs vs Channel Usage of PU.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number 24360147.

References

[1] J.Mitra III, et al, "Cognitive radio: making software radious more personal," IEEE Pers. Commun., vol. 6, no.4, pp.13-18, 1999.

[2] M. Wadhwa, C. Xin, M. Song, and E.K. Park, "Throughput analysis for a contention-based dynamic spectrum sharing model," IEEE Transaction on Wireless Comm., vol.26, no.4, pp.1426-1433, April 2010.

[3] S. Shama, "RSA algorithm using modified subset sum cryptosystem," *IEEE Conference on Computer and Communication Technology (ICCCT)*, pp. 457-461. Sep 2011.

[4] S. Salimi, "Rate regions of secret key sharing in new source model," *IET Communications*, pp. 443-455, March 2011.

[5] D.A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan 1975.

[6] S. Leung-Yan-Cheong, and M. Hllman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform.Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[8] E. Okamoto, "A secure cooperative relay transmission using chaos MIMO scheme," *IEEE ICUF*, pp. 374-378. July 2012.

[9] J. Deng, "Multipath key establishment for wireless sensor networks Using just-enough redundancy transmission," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, pp. 177-190. Sep 2008.

[10] L. Lai, "Secret sharing via noisy broadcast channels," *IEEE ISIT*, pp. 1955-1959. July 2011.

[11] F. Oggir, "The secrecy capacity of the MIMO wiretap channel," *IEEE ISIT*, pp. 524-528, July 2008.