ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

AN EFFICIENT SCHEME FOR CHANNEL UTILISATION IN COGNITIVE RADIO SYSTEMS

Ms. P. KAWYA, IInd ME (Communication System),
Dr. S. KARTHIGAI LAKSHMI, Ph.D., Professor/ECE
SSM Institute of Engineering and Technology, Dindigul, Tamilnadu, India
kawyaece168@gmail.com

ABSTRACT

The cognitive radio (CR) system needs to optimally set the sensing period and sensing time for efficient utilization of the channel while protecting a primary user (PU). The optimal sensing period is used for maximizing the effective throughput of the CR system. It depends on not only the on/off pattern of the PU and the sensing error probabilities but also the size of a data packet, the transmission rate, and the forward error correction capability. In this project, the optimal sensing period is derived mathematically while taking all of these factors into account.On the basis of this optimal period, the sensing scheme for sensing a data packet transmission is proposed. With the proposed sensing scheme, the CR system can protect the PU very well while achieving the high effective throughput and to efficiently utilize the channel.

1. Introduction

1.1 Cognitive Radio Networks

A cognitive radio is an intelligent radio that can be programmed and configured dynamically. Its transceiver is designed to use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in a given spectrum band at one location. This process is a form of dynamic spectrum management. In response to the operator's commands, the cognitive engine is capable of configuring radio-system parameters. These parameters include "waveform, protocol, operating frequency, and networking". This functions as an autonomous unit in the communications environment, exchanging information about the environment with the networks it accesses and other cognitive radios (CRs). A CR "monitors its own performance continuously", in addition to "reading the radio's outputs"; it then uses this information to "determine the RF environment, channel conditions, link performance, etc.", and adjusts the "radio's settings to deliver the required quality of service subject to an appropriate combination of user requirements, operational limitations, and regulatory constraints".

Some "smart radio" proposals combine wireless mesh network— dynamically changing the path messages take between two given nodes using cooperative diversity; cognitive radio—dynamically changing the frequency band used by messages between two consecutive nodes on the path; and software-defined radio—dynamically changing the protocol used by message between two consecutive nodes. Although cognitive radio was initially thought of as a software-defined radio extension, most research work focuses on spectrum-sensing cognitive radio. The chief problem in spectrum-sensing cognitive radio is designing high-quality spectrum-sensing devices and algorithms for exchanging spectrum-sensing data between nodes. It has been shown that a simple energy detector cannot guarantee the accurate detection of signal presence, calling for more sophisticated spectrum sensing techniques and requiring information about spectrum sensing to be regularly exchanged between nodes. Increasing the number of cooperating sensing nodes decreases the probability of false detection. Filling free RF bands adaptively, using OFDMA, is possible approach applications of spectrum-sensing cognitive radio include emergency-network WLAN higher throughput and transmission distance extensions. The evolution of cognitive radio toward cognitive networks is underway; the concept of cognitive networks is to intelligently organize a network of cognitive radios.

2. Related Work

There is a body of research focused on designing secure PIN-entry schemes in face of the threat posed by observation attacks [6]. Some research design their solutions secure against a short-term memory attackers, using the fact that the human short-term memory has a limited capacity. In these solutions, the user is requested to give answers to a set of challenges during a login procedure. The authentication scheme is designed in a way that the user can easily respond to the questions, while the cognitive capacity exceeds the attacker (human) memory.

Bianchi et al. proposed a nonvisual unimodal schemes, which uses hidden audio and vibration challenges for userauthentication [7]. In another work by Bianch et al. Spinlock, Colorlock and Timelock schemes that achieve faster times than Spinlock [8], [1]. All three schemes have partial leakage of information in the observation attack. Other solutions assume the existence of stronger attacker that can record the complete login session and try to recover the user's secret PIN/password. All these scheme are not usable in practice since they all take large authentication time.

Designing a scheme secure against even a simple passive attack in a model where the attacker can observe both challenges and responses appears to be challenging [11]. In Cognitive authentication scheme (CAS), a user mentally computes a path formed by his portfolio images, and gives an answer based on that computed path. CAS scheme is vulnerable to SAT solver attacks and an attack based on probabilistic decision tree. The speed of such attacks can be improved in combination with a timing attack. This comes from the fact that not all decision paths are of the same length, what leads to faster or slower user response times. By measuring this time, the attacker can eliminate some of the possible decision paths what can speed up the whole process of finding the user's password.

To speed up the login process while keeping the solution safe against observation attacks, some solutions rely on the presence of secondary-based channels. Kuber and Yu and Sasamoto et. al. [5] use a tactile channel as a secure hidden challenge channel. In VibraPass authentication system user receives hidden challenges via his mobile phone [3]. Hidden challenges are used to avoid possible manipulations by the attacker. The authors mentioned confused waiting as a potential timing attack.

In the Undercover solution the user simultaneously receives a visual challenge and a hidden tactile challenge via a protected channel and authenticates by answering correctly to several challenges. One of authors of Undercover, Hasegawa et. al. proposed two alternative designs to Undercover [4], one of which uses an audio channel as the carrier of the hidden challenges. The proposed solution is prone to intersection attacks. Undercover is also prone to intersection attacks as independently demonstrated in [9] and [11]. This problem can be easily mitigated if challenges are fixed instead of being randomized. Unfortunately, Undercover is not secure in a very strong attacker model where attacker records user's response time [9]. The attack is based on design flaws and exploits human users' nonuniform behavior on how users respond to different challenges.

3. Channel Utilisation Scheme

The cognitive radio (CR) system opportunistically exploits the spectrum bands that are licensed to the primary users (PUs) but are not used at a particular time and a specific geographic location [2]. Since the coexistence of PU and CR users on the same channel may severely degrade the PU performance, the CR system should be able to detect the activation of the PU as fast as possible.The CR system that investigates the existence of the PU on spectrum by sensing is required to frequently sense its operating channel for the fast PU detection. The channel with the short on/off duration of the PU should be frequently sensed for PU protection; frequent sensing on the channel with low PU activity may degrade the performance of the CR system since the CR system usually stops data transmission during sensing. Thus, to efficiently utilize the channel while protecting the PU properly, many CR systems try to set the sensing interval and/or sensing time optimally. In this, a sensing scheduling scheme to increase the channel utilization, by performing the feature detection after alarms are issued several times from energy detection, to avoid the feature detection on a vacant channel is proposed [10]. The CR system maximizes the throughput by determining rate and power jointly while taking the sensing outcome and sensing error probability into account, for given fixed sensing time and period.

If the PU suddenly returns to the channel where a CR node is transmitting a data packet, the data packet may be corrupted during transmission. When all erroneous bits within the received packet cannot be corrected by the CR receiver, the packet should be retransmitted, and in fact, this decreases the effective throughput of the CR system. Thus, when designing a sensing scheduling scheme for maximizing the throughput of a CR system, the transmission errors due to the collision of the PU and the CR users are to be cosidered**.** In this, a problem for determining the optimal sensing period to maximize the effective throughput of a CR system while protecting the PU, where the effective throughput means the average number of data bits successfully transmitted per second is studied. It is obvious that the channel quality in the CR system can get worse abruptly, owing to the unexpected return of the PU, and if this occurs while a CR node is transmitting a data packet, the received packet might include uncorrectable errors.

The CR receiver requests the packet retransmission to the CR transmitter. Thus, the optimal sensing period for maximizing the effective throughput depends not only on the on/off pattern of the PU and the spectrum sensing error probabilities but also on the size of a data packet, data transmission rate, and the forward error correction (FEC) capability. In this, the optimal sensing period while taking all of these factors into account is derived. On the basis of this optimal period, the sensing strategy that can be efficiently implemented within the data transmission framework of the CR node is proposed. With this strategy, since the CR transmitter has the breaks for sensing during a data packet transmission, the PU can be also properly protected. To the best of our knowledge, the study on the optimal sensing period for maximizing the effective throughput of the CR system, while taking account of transmission error bursts due to the sudden return of the PU, has been rarely addressed in the literature to date.

Consider a small CR network operating on one control channel and multiple data channels with a narrow bandwidth. It is assumed that the data channels are licensed to PUs, whereas the CR system will not be disturbed by PUs in accessing the control channel. The control channel is used only to transmit the control packets for reserving or releasing data channels. The CR nodes access the control channel by using a MAC scheme such as CSMA/CA. Each CR node has a transceiver dedicated to the control channel and another transceiver turned to the current operating data channel. Since a CR node always listens to all packets on the control channel with the dedicated transceiver, it can know which channels have not been reserved. The CR node that wants to transmit traffic first should reserve data channels. To this end, the node selects some vacant channels that are not reserved by other CR nodes from a channel pool and transmits the request-to-send (RTS) packet containing a list of these channels through the control channel.

When a CR node listens to the RTS packet destined for itself, the node selects some channels from the channel list within RTS and replies with the clear-to-send (CTS) packet containing the list of selected channels, of which the first becomes the operating channel and the remaining channels are backup channels. Since the on/offǁ duration of the PU on the channel may be short, a pair of CR transmitter and receiver may perform channel switching several times among the reserved channels until they are released. The channel-hopping sequence corresponds to the sequence of the channel list in CTS. Thus, the transmitter and the receiver have a consistent hopping sequence. It is noted that the data channels reserved to a pair of CR transmitter and receiver are not utilized by other CR nodes until the transmitter releases the channels. When the CR transmitter has no more data packets destined for the receiver or its all reserved channels have been occupied by PUs, it releases the reserved data channels by broadcasting a specific control packet through the control channel.

In this the transmission/reception of data packets between a pair of the CR transmitter and receiver on the reserved data channels is focused. Hereafter, in description, a channel means the reserved data channel.At the transmitter; the FEC encoder generates one FEC block from each data packet. To cope with the burst errors caused by the sudden return of the PU to the channel, the FEC block is interleaved. After being interleaved, the symbols within the original FEC block are evenly shuffled across the entire interleaved FEC block. When the size of a data packet is Nb bits and the number of symbols within an FEC block is Nc, the code rate is Nb/Nc. A fixed code rate, which is denoted by rc, is assumed. It is also assumed that the CR transmitter adjusts the symbol transmission rate according to the channel quality, by adopting the continuous-rate M-ary quadrature amplitude modulation. Let$W$ be the channel bandwidth and γ be the received signal-to-noise ratio (SNR). Then, according to the symbol transmission rate on the channel is

$$Rs = W \log2(1 + (-1.5/\ln(5pe))\gamma),\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(1)$$

where pe is the target symbol error rate. The interleaved FEC block is transmitted with the rate of Rs. Then, the transmission time of this block is $(Nb/rc)/Rs$.

The PU suddenly returns to the channel while an interleaved FEC block is being transmitted, the received block may include many erroneous symbol bursts. If the error bursts within the received block are beyond the error correction capability of coding and interleaving, the CR receiver discards the block, and the CR transmitter should retransmit it. This may deteriorate the throughput performance of the CR system. Moreover, the transmission of the CR nodes can disturb the transmission of the PU, and this is much more critical than the performance degradation of the CR system. Thus, it is needed that the CR transmitter senses the channel while transmitting an interleaved FEC block, and if the PU is detected on the channel, it suspends the transmission of the block.Let T and τs denote the length of the sensing interval and the spectrum sensing time, respectively. The CR transmitter senses the channel during τs at the start of each sensing interval and decides the channel state based on its sensing outcome. The sensing interval starting with the sensing outcome of —off will be called the —off sensing interval. It is obvious that the CR transmitter accesses the channel only during off sensing intervals, to preserve the transmission qualities of both the PU and the CR user. When the sensing outcome is —on, the transmitter suspends transmission and performs channel hopping during the corresponding sensing interval. The receiver also, when unable to hear from the transmitter, moves to a new channel according to the predetermined hopping sequence, i.e., the sequence of channels listed in CTS.

Now, the transmission procedure of a data packet is described in more detail. Just after channel reservation, to get the channel quality information for determining the initial symbol transmission rate *Rs*, the CR transmitter transmits a probe packet through the operating channel. Then, the CR receiver measures the received SNR of this packet, γ, and reports it to the transmitter. The CR transmitter determines *Rs* depending on γ and calculates the required number of off sensing intervals, *k*

$=Nb/[(T - \tau s)rcRs]$……………(2)

After generating an interleaved FEC block from a data packet, the CR transmitter transmits the interleaved FEC block during *k* off sensing intervals. When receiving the entire block, the CR receiver performs deinterleaving and decoding for the block. The CR receiver that has successfully decoded the data packet sends an acknowledgement (ACK) packet; if it fails to recover the data packet, the CR receiver replies with a negative-ACK (NAK) packet. In addition, the CR receiver reports the measured SNR of the block to the transmitter, by piggybacking it on the ACK or NAK packet.

When successfully receiving the feedback packet, the CR transmitter newly determines the symbol transmission rate, based on the received SNR value within the feedback packet. It is noted that the CR transmitter usually measures the received SNR of the feedback packet. The CR transmitter that has failed to recover the feedback packet determines the *Rs* at the next transmission, using the received SNR measured for the feedback packet. If the CR transmitter has decoded the ACK packet successfully, it transmits an interleaved FEC block of a new data packet; otherwise, it retransmits the previous block.

4. Optimal Sensing Period For Maximizing Throughput Of CR User

The optimal sensing period for maximizing the effective throughput of the CR user while properly protecting the PU is investigated. As mentioned earlier, the CR transmitter generates an interleaved FEC block (shortly, a block) from a data packet having the fixed size of Nb bits. After determining the transmission rate Rs using γ reported from the CR receiver, the CR transmitter transmits the block at the rate of Rs during k off sensing intervals, where $k = Nb/(T - \tau s)rcRs$. For given Nb, rc, τs, and Rs, determining the optimal k is equivalent to determining the optimal sensing period T. Since Rs depends on γ, the optimal k and the optimal T are also dependent on γ. A —transmission round is defined as the time period from the instant at which the CR transmitter is ready for a block transmission to the instant at which it again becomes ready for transmitting the next block . During a transmission round with k off sensing intervals, let X(k) be the effective throughput and Φ(k) be the ratio of the coexistence time of the CR user and the PU to the total channel reservation time. It is assumed that, for protecting the PU properly, Φ(k) should not be larger than a predefined threshold, ΦTH. Then, the problem that finds k for maximizing the effective throughput with this constraint is formulated as

$K^{*} = \text{argmax}\ \chi\ (k), k \in N$…………..(3.4)

where N denotes the natural number set.

The transmission of a block requiring k off sensing intervals as a discrete time

Markov chain can be modelled by observing the channel at the start of each sensing interval and at the transmission start of feedback packet.

The states are divided largely into two groups of B and A, according to whether the ongoing operation is a block transmission (B) or feedback transmission (A). In the state Bi,m, i indicates whether a PU exists (i = 1) or not (i = 0) on the channel at the beginning of the state, and m means the total number of off sensing intervals until before the state. The state Ai represents the feedback packet transmission on the channel where the PU activity is i. When Sk is a set of all feasible states, Sk={Bi,m,Ai|i∈ {0, 1},m {0, 1, . . . , k−1}}.The transition probability from a state to another, where pf and pd denote the false alarm probability and the PU detection probability of spectrum sensing, respectively. And τe and τa are respectively the processing time of the FEC encoder/decoder and the transmission time of feedback packet. As an example of state transition, it is examined that the transition from B0,m (0 ≤ m < k− 1). Refer for the transition probabilities from other states. If a false alarm is issued from spectrum sensing, the transmitter performs channel hopping. Then, since the new channel after hopping is vacant with probability π0 or has been occupied by a PU with probability π1, the transition probability from B0,m to B0,mis pfπ0, and the transition probability from B0,m to B1,m is pfπ1.

In state B0,m, when a PU detection alarm is not issued, the data block is transmitted until before the next sensing. Since the probability that a PU returns during this interval is ϕ0,1(T), the state transition from B0,m to B1,m+1 occurs with probability (1 − pf)0,1(T). Also, since the probability of a vacant channel during this sensing interval is ϕ0,0(T), the transition probability from B0,m to B0,m+1 is (1 − pf)0,0(T).

5. Performance Analysis

In this the performance of the proposed sensing scheme is evaluated.The used common parameter values as are follows:

$\Phi TH = 10-3$, $\tau s = 0.2$ ms, $\tau a = 5$ ms, $W = 200$ kHz, $pe = 0.001$,
$\tau e = 0.25$ms when $Nb = 8192$, and $\tau e = 1$ ms when $Nb = 32768$.

The (m, n) Hamming code, which encodes n data bits into an m-symbol codeword, and a block interleaver are considered. It is well known that a single bit error can be corrected with a Hamming code. Thus, $rc = n/m$ and $\Lambda TH = 1/(m- 1)$. For checking the validity of analysis, the simulation results are additionally presented. First, the optimal sensing period T^* according to γ is investigated.

It is assumed that an interleaved FEC block is divided into k fragments and is transmitted during k off sensing intervals. As γ increases, since the transmission rate Rs is increased, a fragment can be transmitted during shorter time. Accordingly, the time that a PU and a CR user simultaneously transmit is also decreased with higher γ. This means that a larger fragment can be supported with given error correction capability. Thus, the optimal k is discretely decreased with the increase of γ. Since $T^* = \tau s + Nb/(k^*rcRs)$, as γ increases, T^* is decreased owing to the increase of Rs for the range of γ giving the same k^*; it is sharply increased whenever the value of k^* is decreased. Since the proposed scheme determines the sensing period so that the block retransmission is minimized, the increase of Rs due to higher γ leads to the increase of the throughput and the shorter transmission round. In addition, it is observed that the longer $T0$ leads to the longer sensing interval. This is because the CR transmitter can utilize the channel more stably with the longer $T0$. In turn, this results in the higher throughput and the shorter transmission round. The influence that a data packet size and a code rate have on the sensing period, the throughput, and the transmission round length. The same code rate, the CR transmitter can adopt the longer sensing interval while transmitting the longer data packet. This is because, with the longer data packet, the symbols within a codeword are farther from each other after interleaving.

Also, the throughput performance is naturally improved with the longer sensing interval, i.e., with the longer data packet, owing to the smaller sensing overhead. On the other hand, with the higher ΛTH, the CR transmitter has the longer sensing interval because more corrupted symbols within an FEC block can be allowed. Accordingly, the optimal sensing period is longer when ΛTH = 1/4 than when ΛTH = 1/14. In addition, for the same size of a data packet, the throughput performance gets worse, and the transmission round gets longer with the lower code rate, since the larger FEC block should be transmitted .The proposed scheme achieves a high throughput performance while protecting the PU very remarkably, by allowing the breaks for sensing during a block transmission.

Parameters	**Values**
N_b(bit rate)	32678
P_d(detection probability)	0.9900
P_f(Feedback failure probability)	0.1000
r_c(Code rate)	3.7500
R_s(Transmitter block rate)	7.1929e0.4
τ_e(Sensing time)	1.0000e-03
T_o(Optimal sensing period)	4

Table 5.1 Numerical Results

6. Conclusion and Future Work

In this project the optimal sensing period has been derived on the basis of the size of the data packet, transmission rate and forward error correction capability. Based on this optimal period, the sensing scheme for data packet transmission is proposed. With this sensing scheme, the cognitive radio protects the primary user very well and high effective throughput is achieved and hence the channel is efficiently utilized. In the future, this work can be extended for variable time sensing scheme for multi user and the throughput can be increased further more.

References

[1] A. Bianchi, I. Oakley, and D. S. Kwon, “Spinlock: A single-cue haptic and audio PIN input technique for authentication,” in *Haptic and Audio Interaction Design*, vol. 6851. Berlin, Germany: Springer-Verlag, 2011, pp. 81–90.

[2] Mario Cagalj, Toni Perkovi´c and Marin Bugari, “Timing Attacks on Cognitive Authentication Schemes”, IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015

[3] A. De Luca, E. von Zezschwitz, and H. Hußmann, “Vibrapass: Secure authentication based on shared lies,” in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, 2009, pp. 913–916.

[4] M. Hasegawa, N. Christin, and E. Hayashi, “New directions in multisensory authentication,” in *Proc. 7th Int. Conf. Pervasive Comput. (Pervasive)*, 2009, pp. 103–106.

[5] H. Sasamoto, N. Christin, and E. Hayashi, “Undercover: Authentication usable in front of prying eyes,” in *Proc. Conf. Human Factors Comput. Syst. (CHI)*, 2008, pp. 183–192.

[6] A. De Luca, K. Hertzschuch, and H. Hussmann, “ColorPIN: Securing PIN entry through indirect input,” in *Proc. CHI*, 2010, pp. 1103–1106.

[7] A. Bianchi, I. Oakley, and D. S. Kwon, “The secure haptic keypad: A tactile password system,” in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, 2010, pp. 1089–1092.
[8] A. Bianchi, I. Oakley, and D. S. Kwon, “Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry,” *Interact. Comput.*, vol. 24, no. 5, pp. 409–422, 2012.
[9] T. Perkovic, S. Li, A. Mumtaz, S. A. Khayam, Y. Javed, and M. ˇ Cagalj, “Breaking undercover: Exploiting design flaws and nonuniform human behavior,” in *Proc. 7th Symp. Usable Privacy Secur. (SOUPS)*, 2011, Art. ID 5.
[10] M.-K. Lee, “Security notions and advanced method for human shouldersurfing resistant PIN-entry,” *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 695–708, Apr. 2014.
[11] Q. Yan, J. Han, Y. Li, and R. H. Deng, “On limitations of designing leakage resilient password systems: Attacks, principals and usability,” in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2012.