Collaborative Anti-jamming Broadcast with Uncoordinated Frequency Hopping over USRP

Guiquan Chen, Yan Li, Liang Xiao, Lianfen Huang
Dept. of Communication Engineering, Xiamen University, 361005, China

***Abstract*—Cognitive radio networks (CRNs) are threatened by smart jammers that aim to block the ongoing transmissions of secondary users according to their transmission patterns obtained from public control channels or compromised secondary users. Without requiring any pre-shared PHY-layer keys at the receivers, the uncoordinated frequency hopping (UFH) technique that was proposed to address smart jammers suffers from a low communication efficiency. In this paper, we develop a UFH-based collaborative broadcast system over universal software radio peripherals (USRPs), which exploits the node cooperation to improve the broadcast efficiency and jamming resistance of CRNs. Experiments are performed over USRPs to evaluate the broadcast performance against smart jammers under various network topologies. We investigate the impact of the CRN bandwidth, the prediction accuracy of smart jammers regarding the CRN frequency hopping pattern, and the jamming power and signal pattern. Experimental results show that the proposed broadcast system is more robust than three benchmark broadcast systems in most jamming scenarios.**

I. Introduction

Anti-jamming broadcast is critical for security sensitive services in cognitive radio networks (CRNs), where a source node aims at sending a broadcast message to all the receivers (RXs) in the presence of one or multiple jammers [1], [2]. Widely used to counteract jamming attacks, the frequency hopping (FH) technique requires that all the RX nodes know the FH pattern of the source node and this PHY-layer secret has to be protected from jammers. Unfortunately, smart jammers utilize this fact to improve the jamming strength [3]–[6]. As a type of reactive jammers that sense the spectrum before jamming, smart jammers can not only block the target channels with flexible power, but also eavesdrop the public control channels and compromise some RX nodes in a large-scale CRN to derive the FH patterns of the source node, yielding failed transmissions of the CRN thereafter.

The uncoordinated frequency hopping (UFH) technique [7] and its variations [8]–[13] were proposed to address smart jammers. Without requiring any pre-shared FH pattern, an UFH-based receiver randomly selects a channel from the public channel set. A packet can be successfully received if both the transmitter and the receiver come across the same unblocked channel, indicating a very small packet reception rate due to the large number of channels of UFH to counteract jamming. Therefore, a collaborative UFH-based broadcast (CUB) strategy exploits the node cooperation to provide the spatial and spectrum diversity and thus enhance the communication efficiency of UFH and its broadcast performance has been preliminarily evaluated via simulations in [14].

To further study the collaborative UFH-based broadcast, in this paper, we propose a UFH-based anti-jamming collaborative broadcast in cognitive radio networks (UCBC), where the secondary users (SUs) that have successfully received the broadcast message relay it to increase the successful reception rate of the other SUs. The channel selection of the relay SUs has to ensure the uninterrupted transmission of primary users (PUs) in the CRN. By exploiting both the frequency diversity and spatial diversity of the cognitive radio network, this technique can achieve stronger jamming resistant and higher communication efficiency than most recent attempts for anti-jamming broadcast. This broadcast scheme as well as the smart jammer is implemented over the universal software radio peripherals (USRP) and GNU Radio platform, and field tests have been performed to investigate their performance under various scenarios.

The performance of UCBC is evaluated with experiments in terms of the broadcast delay and the overall energy consumed by the USRPs during the whole broadcast process. Unlike existing related work on UFH, our experiments have been performed using a powerful smart jammer in more complete jamming scenarios. To the best of our knowledge, this paper is the first to consider the incomplete hopping pattern in FH, UFH and their variations and demonstrate its feasibility by a prototype implementation on a software-defined radio platform. Note that smart jammers can obtain part of the FH pattern of the transmission that is sent over the control channel to the receivers in the whole CRN using the coordinated FH. For example, a jammer usually misses blocking some packets due to an inaccurate or delayed knowledge on the FH pattern of SUs, which results from the channel fading and the delay to decode the FH pattern.

The performance of UCBC is evaluated via experiments performed in various cognitive radio networks against smart jammers implemented over USRP. We investigate smart jammers with various abilities to sense and block the channels, as well as the accuracy to retrieve the PHY-layer secret by eavesdropping and compromising the CR nodes, and evaluate the impact of the estimation error of smart jammers on the broadcast performance.

The remainder of this paper is organized as follows. We describe smart jamming in Section II, and present the UFH-

The work of L. Xiao was partly supported by NSFC (61271242).

978-1-4799-8088-8/15/$31.00 ©2015 IEEE

based collaborative broadcast system over USRP in Section III. In Section IV, experimental results are provided to evaluate the performance of UCBC against smart jammers in CRN. Finally, we conclude this paper in Section V.

II. Smart Jamming in Cognitive Radio Networks

Jammers aim to block the ongoing local transmission by injecting jamming signals on the same channel with the current transmitter with high power. The resulting low signal-to-noise-plus-interference-ratio (SINR) at the receiver yields a packet loss. With limited computation and transmission capability, a jammer blocks the channels that are most likely to carry out the target packets to its own illegal interests. Thus, reactive jammers sense the ongoing spectrum usage before selecting their targeted channels and thus significantly save the jamming power and have been shown to be much more powerful than non-reactive jammers such as static jammers.

As an advanced type of reactive jammers, smart jammers have been developed in recent years and are capable of throwing serious attacks to cognitive radio networks [15]. Smart jammers are especially powerful to the coordinated FH system, in which the source node declares its transmission channel pattern to the RX nodes in advance. More specifically, by eavesdropping the control channel and corrupting the RX nodes in a mobile large-scale wireless network, smart jammers have a chance to retrieve the FH pattern and then block all the following transmissions.

Equipped with USRP/GNU Radio platforms, smart jammers aim to block the broadcast messages, increase the broadcast delay, and energy costs of SUs. A smart jammer first attacks the control channel and/or corrupts the CR nodes to obtain the FH pattern, which is sometimes inaccurate due to the propagation loss in distributed CRNs. Let P_e represent the estimation error rate of a smart jammer. In the coordinated FH-based system, the accuracy of this information to the jammer impacts on the performance of the broadcast. On the other hand, as the FH pattern of the source node is hidden in the UFH-based system, a smart jammer cannot obtain the PHY-layer key by eavesdropping, and thus have to block the broadcast by brutally forcing. Assume a jammer can sense and block C_J channels in each time slot in hopes of coming across the packet from the C channels. In this case, the probability of a packet to be blocked is C_J/C. Let p as the probability for a jammer to block the right channel, which is given by

$$p = \begin{cases} \max\left(1 - P_e, \frac{C_J}{C}\right), & \text{FH} \\ \frac{C_J}{C}, & \text{UFH} \end{cases}, \tag{1}$$

where $p = 1$ corresponds to the case that a jammer can obtain the exact channel information for coordinated FH-based scheme or block all the C channels all the time for UFH-based and FH-based scheme. However, for the limited of energy and jamming bandwidth, the jammer can not keep jamming a large number of channales, i.e. $C_J \ll C$. We aim to design a broadcast scheme in CRN to reduce the broadcast delay and the overall energy consumption to complete the message broadcast in the presence of smart jammers.

III. Collaborative anti-jamming broadcast communication using UFH

We proposed a UFH-based collaborative broadcast in CRN (UCBC) to counteract smart jammers without preshared any PHY-layer keys in this section. We first present the basic concepts of UCBC scheme and then provide details of our USRP-based testbed which designed to evaluate the performance of UCBC under different jamming scenarios.

A. UFH-based collaborative broadcast in CRN

The existing UFH-based broadcast schemes suffered from low communication efficiency in CRN for the randomly channels selection from a large number of temporarily-unused licensed channels. We concentrate on the activities of the SUs and propose a UFH-based collaborative broadcast in CRN to provide an anti-jamming broadcast scheme without preshared any secret keys.

The main idea of UCBC is to exploit the RX node cooperation to enhance both the communication efficiency and system security. More specifically, the RX nodes that already obtain the broadcast message relay it to their neighboring RX nodes. In this UFH-based process, the RX nodes do not have any pre-shared PHY-layer keys, i.e., the frequency hopping pattern of the source node. Consequently, the broadcast cannot be completely blocked by smart jammers.

In UCBC system, the source node sends the M packets of the broadcast message sequentially and repeatedly according to a certain frequency hopping pattern. Without knowing this pattern, each SU RX node randomly selects a channel in each time-slot and receives a broadcast packet if the channel is not jammed and carries the packet sent by the source node or a relay node.

Relay SUs have to stop broadcasting after a sufficiently long time to increase the reception rate of the neighboring SUs and to avoid energy waste. In UCBC, a relay node stops sending packets once receiving ACKs from all of the neighboring SU RX nodes. As the degradation of wireless channel and interference may result in the loss of the ACK signals, the maximum transmission duration is used to stop relay. Therefore, a SU stops broadcasting once receiving all the ACKs or reaching the maximum transmission duration Δ, whichever comes first.

Assume that the source node periodically broadcasts *M* short packets to *L* SUs within its communication range. Let $p_a = (1-p)/C$ be the successful packet reception rate of a SU, and thus the probability for all these *L* SUs to receive *M* packets during the first *n* slots is given by

$$P[n] = (1 - (1 - p_a)^n)^{ML}. \tag{2}$$

According to the analysis in [7], the average broadcast delay can be written as

$$T = M \sum_{n=0}^{\infty} (1 - (1 - p_a)^n)^{ML}. \tag{3}$$

For the various scenarios, α have been defined as a parameter which can be fine tuned in practice according to the need, if

jamming is particularly a concern, α can set to a larger value. The communication duration Δ is given by

$$\Delta = \alpha T = \alpha M \sum_{n=0}^{\infty} (1-(1-p_a)^n)^{ML}. \quad (4)$$

B. Implementation on USRPs

We implemented the proposed broadcast system over USRPs. Each broadcast message is split into M short fragments of the same length, denoted as F_i, $1 \leq i \leq M$. The source node encapsulates fragment F_i into packet m_i, which includes the fragment number (i), the number of the packets (M) and fragment (F_i). These M packets are modulated with Gaussian minimum shift keying (GMSK) and transmitted periodically and repeatedly on the channels randomly chosen from $C = 256$ channels ranging between 2.302 GHz and 2.814 GHz.

The block diagram of a RX node in the USRP-based UCBC system is shown in Fig. 1, which consists of a receiving mode and a relay mode that are managed by a UCBC controller following Algorithm 1. The receiving mode is made up of the decoder, demodulation, information extraction and a channel randomly selected from C. In the broadcast, each RX node first enters the receiving mode. After successfully receiving the M packets, the RX node sends an ACK signal that includes its node ID and times tamps on the control channel and then enters the relay mode for the proposed UCBC and turn to end for the non-collaborative broadcast based on UFH (NBU).

In each time-slot during the relay mode, the node extracts a received packet from the buffer and transmits it at a selected channel unknown to its neighbors based on the same encoding and modulation schemes as the source node. Then the node chooses another channel to send the next packet and the process repeats until the relay mode stops. As benchmark, we also implement the collaborative broadcast of FH (CBFH) and the non-collaborative broadcast based on FH (NBFH) over USRP.

We compute the broadcast delay t_s, which defined as the duration from the beginning of broadcast till all three SU RX nodes have successfully received the broadcast message. The corresponding energy consumption E_t denotes the energy consumed by the source node and the SU RX nodes at receiving mode and relay mode during the whole transmission process, thus we have $E_t = t_s p_{tx} + \sum_{i=1}^{N} (p_{rx} t_{rx}^i + p_{re} t_{re}^i)$, where t_{rx}^i and t_{re}^i denote the time duration for the i-th SU RX node to receive and relay the message, P_{tx}, P_{rx} and P_{re} denote the power consumed by the source node at transmission mode, the SU Rx node at receiving mode and relay mode, respectively.

IV. Experimental Results

Experiments have been performed to evaluate the performance of the USRP-based UCBC broadcast against smart jammers with various jamming strengths in a $7 \times 8 \times 3$ m^3 office room. For comparison, we implemented the collaborative broadcast of frequency hopping (CBFH) and the non-collaborative broadcast based on FH (NBFH) [16] and UFH (NBU) [7].

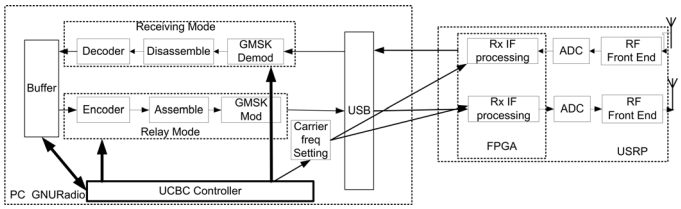


Fig. 1. Block diagram of a secondary user in the UFH-based collaborative broadcast system.

Algorithm 1 UCBC controller algorithm

```
while all M packets are obtained do
    Listen to a randomly selected channel from C
    if receive a new packet then
        store the packet
    end if
end while
Send ACK (Message ID, Node ID, Time Stamp)
while received ACKS ≤ N ≤ Δ do
    Read the next packets from buffer
    Send packet on a randomly selected channel
end while
```

It is challenging even for smart jammers to obtain in time the accurate FH pattern of the source node by eavesdropping the public control channel, if such information exists. Thus we use the jamming probability in Eq. 1 to investigate the impacts of jammer's uncertainty about the source node FH pattern on the broadcast performance, including the broadcast delay, corresponding overall energy consumption and the successful packet reception rate.

A. Experimental Settings

As shown in Fig. 2, each SU or smart jammer in the anti-jamming broadcast testbench consists of a laptop with Ubuntu and GNU Radio and a USRP board with two RF2400 daughter-boards operating over the spectrum from 2.3 to 2.9 GHz. Experiments were performed with network topology as shown in Fig. 3, in which a source node broadcasted a message consisting of $M = 5$ short packets to $N = 3$ SUs against several smart jammers. Each experiment was performed 50 times at different time for each scenario, in which each packet has 512 bytes, the transmission time $T_s = 1$ s, the jamming power $-43 \leq P_J \leq -23$ dBm , the estimation error rate of a smart jammer $0 \leq P_e \leq 0.09$, $1 \leq C_J \leq 64$, and $C = 128$, if not specified otherwise. The experimental results can be viewed as a lower-bound of the broadcast performance against jamming.

B. Experimental Results

In Experiment 1, the proposed broadcast system was evaluated under Topo #1, against a smart jammer with $2 \leq C_J \leq 64$, $0 < P_e \leq 0.09$, and $P_J = -23$ dBm. As shown in Fig. 4,

Fig. 2. Broadcast testbench consisting of USRP-based CR nodes and smart jammers.

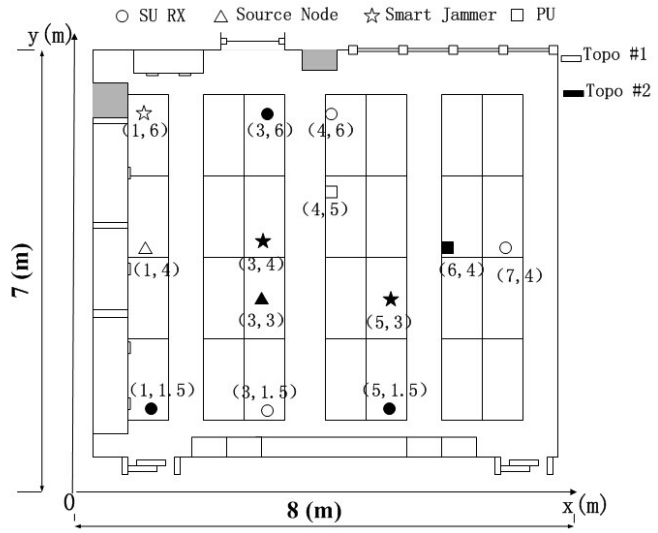


Fig. 3. Network topologies of experiments performed in an indoor lab $7 \times 8 \times 3$ m^3, including a source node, up to 2 smart jammers and 3 SUs to receive the broadcast message in four experiments.

the broadcast delay of NBFH increases from 101 to 885, as P_e decreases from 0.09 to 0.01. The broadcast delay of UCBC is less than the FH-based broadcast schemes if $P_e \leq 0.065$ and outperforms the other three schemes in most cases. As shown in Fig. 5, UCBC resists the smart jammer betters than the FH-based schemes, if $C_J < 50$.

In Experiment 2, two network topologies were evaluated with $C_J = 5$, $P_e = 0.05$ and $16 \leq C \leq 64$. It's obvious that Topo #2 has the stronger jamming strength compared to Topo #1. As shown in Fig. 6(a), UCBC take the minimum time to complete the broadcast compared to the other three broadcast schemes under both the Topo #1 and Topo #2. Another interesting observation is that the cooperation performance of UCBC is better under Topo #2 than Topo #1. For example, compared to the corresponding non-collaborative broadcast scheme (NBU), UCBC takes only 66% of the time to complete the broadcast under Topo #2, and 72% under Topo #1, with $C = 128$. Hence, the saving in broadcast delay by replacing NBU with UCBC is more prominent in a strong jamming network.

Next, as shown in Fig. 6(b), the overall energy consumed by UCBC is also less than the other three schemes. In addition,

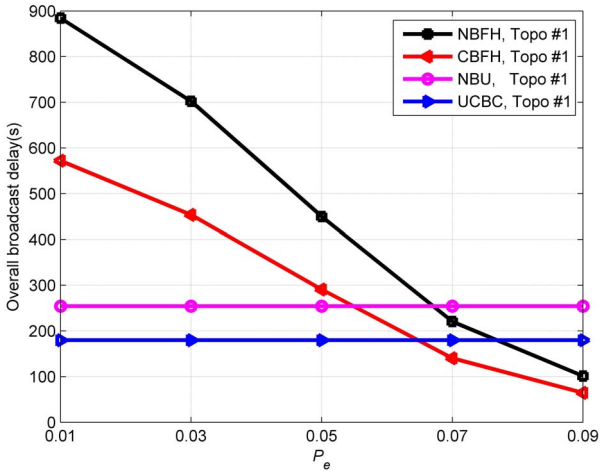


Fig. 4. Overall broadcast delay in presence of a source node broadcasts $M = 5$ packets to $N = 3$ nodes under Topo #1, smart jammer with C_J = 5, P_J = -23 dBm, and $0 < P_e \leq 0.09$.

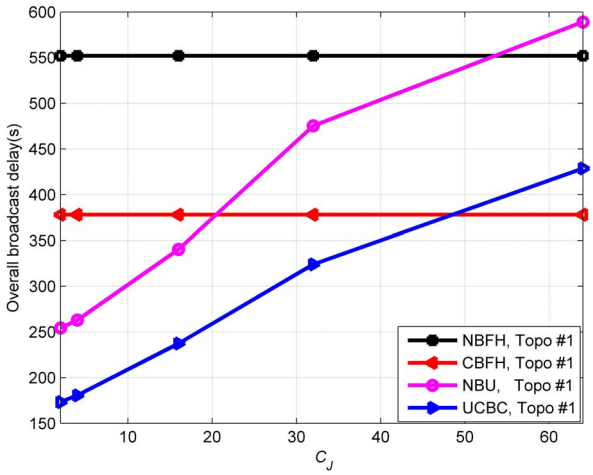
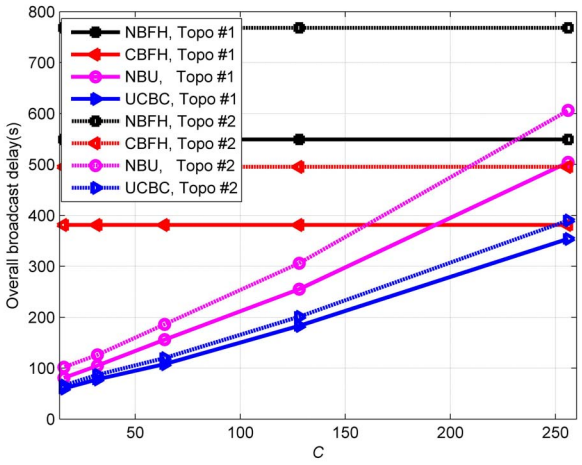


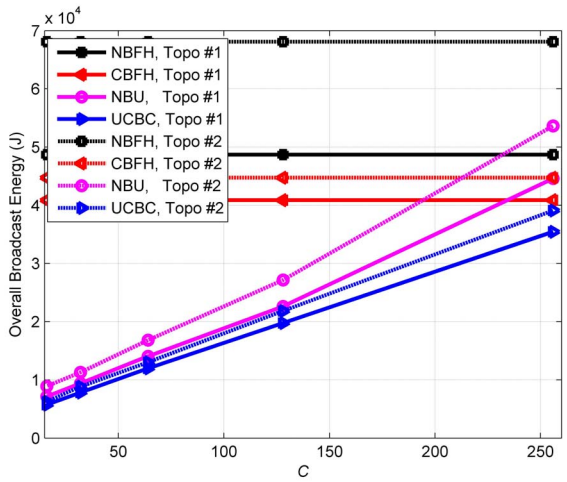
Fig. 5. Overall broadcast delay of UCBC, in which a source node broadcasts $M = 5$ packets to $N = 3$ nodes under Topo #1 against a smart jammer with P_e = 0.04, P_J = -23 dBm, and $2 < C_J \leq 64$.

due to the energy costs of relay nodes, the benefit of node cooperation in terms of the overall energy consumption is smaller than the performance gain in terms of the broadcast speed. However, node cooperation still saves energy, e.g., UCBC consumes about 82% energy compared with the NBU system in the presence of 2 jammers.

In Experiment 3, two jamming signal patterns were evaluated, in which the source node broadcasts 1000 packets under Topo #2, and the process repeats 100 times. As shown in Fig. 7, the proposed UCBC has a larger successful packet reception rate than other three types of broadcast schemes, with jamming signals in both square waves and sinusoids. In addition, the average packet reception rate for the proposed UCBC scheme decreases 27.9%, if the jammer use square wave instead of



(a) Broadcast delay



(b) Overall energy consumption

Fig. 6. Broadcast performance under two network topologies, in which a source node broadcasts M = 5 packets to N = 3 nodes, with P_e = 0.04, C_J = 5 and the number of channels C ranging between 16 and 256.

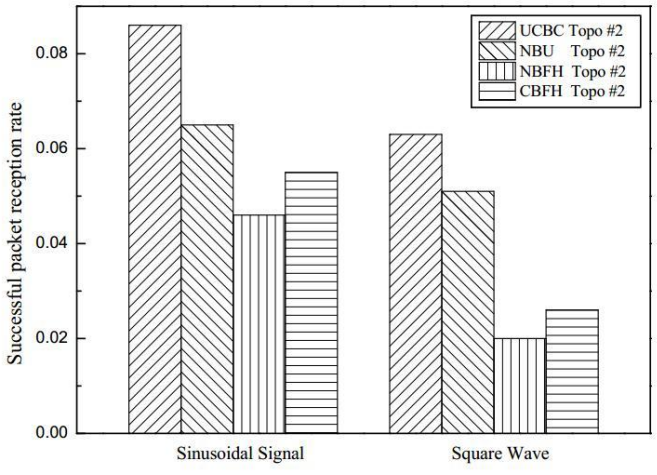
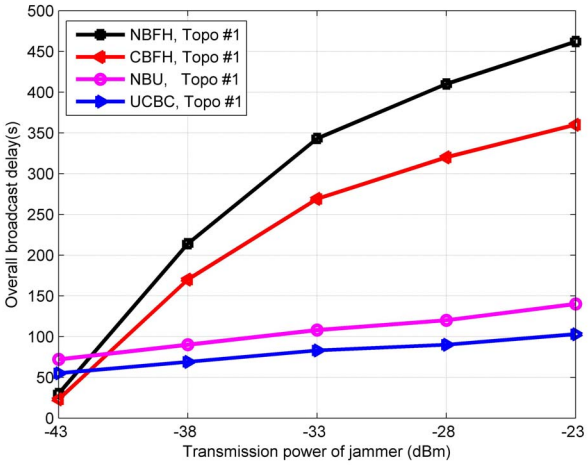
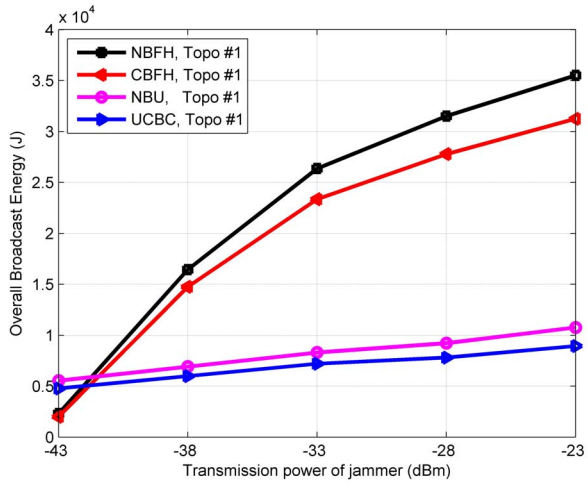


Fig. 7. Successful packet reception rate, with $C_J = 2$, $P_e = 0.01$ and $C = 128$ under Topo #2.



(a) Broadcast delay



(b) Overall energy consumption

Fig. 8. Broadcast performance under under Topo #1, in which a source node sends M = 5 packets to N = 3 nodes against a smart jammer with C_J = 1, P_e = 0.075, and the transmission power ranging from -43 to -23 dBm.

sinusoidal signal.

Finally, in Experiment 4, the transmit power of smart jammer (P_J) range from -43 dBm to -38 dBm and is not high enough to reach the whole network. We alter P_J and calculate the corresponding overall broadcast delay and energy consumption under Topo #1. The overall broadcast delay and energy consumption for the four broadcast schemes are depicted in Fig. 8, with $C = 128$, $C_J = 1$, $P_e = 0.75$ and $-43 < P_J \leq -23$. The performance of UFH-based broadcast schemes degrade more gracely than FH-based schemes. For instance, with P_J increases from -43 dBm to -23 dBm, the broadcast delay for UCBC and NBFH increase 2 and 15 times, respectively. The proposed UCBC exceeds the other three broadcast schemes if $P_J > -42$ dBm.

V. Conclusion

In this paper, we have designed and implemented a UFH-based collaborative broadcast system over USRP to resist jamming in cognitive radio networks. Experiments have been performed to evaluate the performance of the proposed broadcast system against smart jammers with various jamming strengths and signal patterns, showing that UCBC can significantly reduce the broadcast delay and energy against smart jammers compared with the other broadcast systems. For example, UCBC saves 67% of the time and 58% of the energy compared with the traditional FH-based broadcast in a scenario consisting of three cognitive radio nodes and a smart jammer with 16 MHz jamming bandwidth and estimation accuracy of 99.5% regarding the ongoing frequency hopping patterns of the CRN. In addition, in a multi-hop cognitive radio network with two smart jammers, UCBC saves about 34% of the time than the UFH-based broadcast without node cooperation.

References

[1] G. Yue and X. Wang, "Anti-jamming coding techniques with application to cognitive radio," *IEEE Trans. Wireless Communications*, pp. 5996–6007, 2009.

[2] W. Cadeau and X. Li, "Anti-jamming performance of cognitive radio networks under multiple uncoordinated jammers in fading environment," in *Proc. IEEE Annual Conference on Information Sciences and Systems*, pp. 1 – 6, 2012.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 46–57, 2005.

[4] L. Baird, W. Bahn, M. Collins, M. Carlisle, and S. Butler, "Keyless jam resistance," in *Proc. IEEE Information Assurance and Security Workshop*, pp. 143–150, 2007.

[5] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in *Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 169–180, 2009.

[6] A. Cassola, T. Jin, G. Noubir, and B. Thapa, "Efficient spread spectrum communication without pre-shared secrets," *IEEE Trans. Mobile Computing,*, vol. 12, no. 1, pp. 1669 – 1680, 2013.

[7] M. Strasser, S. Capkun, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE Symposium on Security and Privacy*, pp. 64–78, 2008.

[8] A. Liu, P. Ning, H. Dai, and Y. Liu, "USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure," in *Proc. IEEE International Conference on Mobile Adhoc and Sensor Systems*, pp. 41–50, 2010.

[9] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, 2010.

[10] Q. Wang, P. Xu, K. Ren, and X. Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE J. Selected Areas in Communications*, vol. 30, no. 1, pp. 16–30, 2012.

[11] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast in wireless networks, Part I: Single-hop networks," in *Proc. IEEE Global Telecommunications Conference*, pp. 1 – 6, 2011.

[12] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast in wireless networks, Part II: Multihop networks," in *Proc. IEEE Global Telecommunications Conference*, pp. 1 – 6, 2011.

[13] J. Liu, L. Xiao, Y. Li, and L. Huang, "User-centric analysis on jamming game with action detection error," in *Proc. IEEE International Conference on Game Theory for Networks*, pp. 120–125, 2014.

[14] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 297–309, 2012.

[15] D. Yang, G. Xue, J. Zhang, and X. Fang, "Coping with a smart jammer in wireless networks: A stackelberg game approach," *IEEE Trans. Wireless Communications*, pp. 4038–4047, 2013.

[16] C. Li, H. Dai, L. Xiao, and P. Ning, "Analysis and optimization on jamming-resistant collaborative broadcast in large-scale networks," in *Proc. IEEE Asilomar Conference on Signals, Systems and Computers*, pp. 1859 – 1863, 2010.