# Vulnerabilities of Cognitive Radio MAC Protocols and Countermeasures

Yan Zhang and Loukas Lazos
Dept. of Electrical and Computer Engineering, University of Arizona
Email: yanzhang@email.arizona.edu, llazos@ece.arizona.edu

***Abstract*—Cognitive Radio (CR) is a promising technology for opportunistically accessing underutilized licensed spectrum to achieve higher spectrum efficiency and communication throughput. These performance gains are contingent upon the efficient coordination of channel access to the idle portion of the spectrum, an operation performed at the Medium Access Control (MAC) layer. In this article, we identify various vulnerabilities of state-of-the-art CR MAC protocols, exploited by selfish/malicious CR users for gaining an unfair share of the available network resources. Furthermore, possible countermeasures for detecting and mitigating these vulnerabilities are discussed.**

***Index Terms*—Security, cognitive radio networks, MAC, misbehavior, jamming, denial-of-service.**

## I. Introduction

With the proliferation of numerous wireless technologies, the current practice of licensing the available spectrum for exclusive use has led to severe spectrum scarcity. At the same time, most of the licensed spectrum is underutilized. To address spectrum scarcity, an alternative policy of opportunistic access to vacant portions of the licensed spectrum is being pursued. Under this policy, a two-tier network architecture is established. Network users are classified to primary if they are licensed to operate on a particular band, and secondary if they can only access that band when it is free of primary user (PU) activity.

Cognitive Radio (CR) is a promising enabling technology for realizing opportunistic spectrum access. CR devices are capable of sensing and coordinating access to the idle portion of the spectrum, while not interfering with PU activity. A general CR system model is depicted in Fig. 1. The basic functions of a CR system include spectrum sensing, spectrum management, and spectrum access. In spectrum sensing, CRs use signal detection techniques such as energy detection, matched filtering, and cyclostationary feature detection to independently determine the set of idle channels. To combat errors due to shadowing and fading, cooperative sensing is employed. CRs share their sensing observations using explicit messaging over a control channel or by transmitting busy tones on pre-specified frequencies. The sensing observations are fused to reliably determine the idle portion of the spectrum. Information fusion is either centralized or decentralized and the decision rules are based on soft or hard decision combining.

The spectrum management function allocates the idle spectrum to competing CRs. Spectrum allocation can be centrally performed by the fusion center or be coordinated in a distributed manner. Finally, spectrum access is mediated at the Medium Access Control (MAC) layer, which is designed to dynamically allocate the set of idle channels among CRs. To this end, several CR MAC designs that manage access to idle channels have been proposed [1]–[5]. Typically, these designs integrate the functions of spectrum sensing, spectrum information sharing and spectrum access.

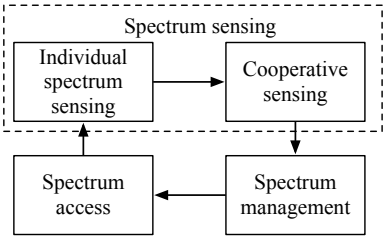


Fig. 1. A general CR system model.

Cooperative CR MAC protocols are designed to provide fair access opportunities to all participating CRs, if CRs remain protocol-compliant. However, selfish or malicious CRs violating the CR MAC protocol specifications can gain an unfair share of the idle spectrum (selfish), or deny spectrum access to other CRs (malicious). Such selfish or malicious activities could significantly degrade the performance of CR networks, or render them inoperable for large periods of time.

In this article, we identify vulnerabilities of state-of-the-art CR MAC protocols. We categorize these vulnerabilities to three classes: (a) attacks on spectrum sensing, (b) attacks on the channel negotiation process, and (c) denial-of-service attacks. For each class, we present possible countermeasures. The remainder of this article is organized as follows: Section II describes state-of-the-art CR MAC protocols. In Section III, we identify CR MAC vulnerabilities. Possible countermeasures are presented in Section IV. In Section V, we discuss further challenges in securing CR MAC protocols.

## II. CR MAC Protocols

CR MAC protocols can be classified into three categories: (a) split-phase, (b) dedicated control channel, and (c) frequency hopping. In this section, we describe the operational features of each of the three classes.

### A. Split-phase CR MAC Protocols

In split-phase CR MAC protocols, time is divided to alternating control and data phases. CRs coordinate access to the idle channels during a control phase, before engaging to data transmissions [1], [2]. The control phase is further divided to a spectrum sensing, spectrum information sharing,

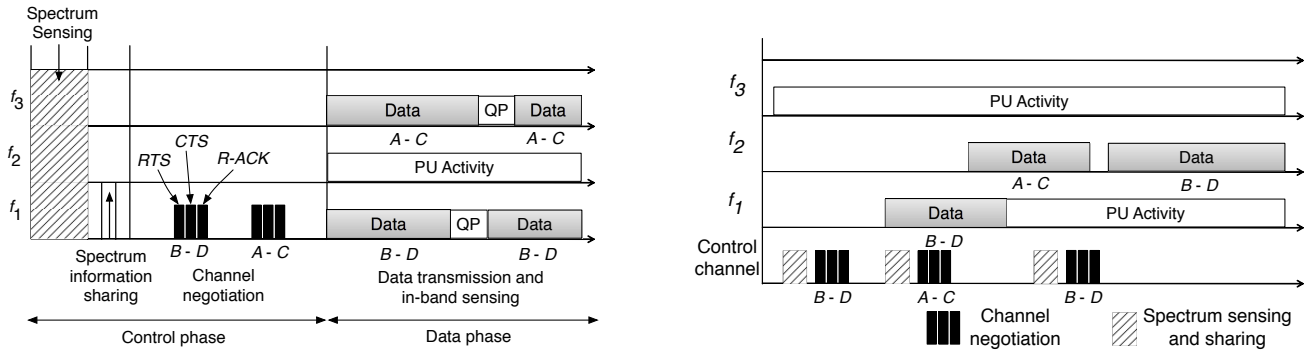


Fig. 2. (a) Alternating control and data phases for a split-phase CR MAC. During the control phase, CRs sense for idle channels and share their sensing observations by transmitting busy tones on dedicated time slots. CRs negotiate the spectrum allocation for the upcoming data phase. In the data phase, CRs switch to the negotiated channels. In-band sensing is performed to avoid interference with PUs, (b) a dedicated control channel CR MAC protocol. CRs perform spectrum sensing, information sharing, and channel negotiations on a dedicated channel while engaging in data transmissions on other channels.

and channel negotiation phase. During the spectrum sensing phase, CRs individually sense the set of idle channels. The sensing observations are shared during the spectrum information sharing phase by converging to a common control channel. The control phase is completed with the channel negotiations for the upcoming data phase. In the data phase, CRs switch to the agreed channels.

In MMAC-CR [1], sensing information is shared by transmitting busy tones. The spectrum information sharing phase is divided to a fixed number of slots 1,...,$k$, equal to the number of potentially available bands $f_1$,...,$f_k$. If any of the CRs transmits a busy tone at slot $i$, channel $f_i$ is assumed to be occupied by a PU. CRs negotiate the channel assignment using a variant of the Distributed Coordination Function (DCF) of IEEE 802.11. When a CR has a packet to transmit, it waits for a random backoff time before transmitting a request-to-send (RTS) packet to a desired receiver. The RTS contains the list of idle channels at the sender in the order of preference. The backoff value is selected within the interval $[0, CW]$, where $CW$ denotes the CR's current contention window (CW) size. The CW is initially set to $cw_0$ (minimum CW) and is doubled with every retransmission up to $cw_{max}$. A receiver of an RTS, combines the preference list of the sender with its own, and replies with a clear-to-send (CTS) message that reserves the channel with the least number of reservations. CRs around the receiver overhearing the CTS update their channel preference list by degrading the priority of the selected channel. The sender confirms the receiver's channel selection by corresponding with a reservation acknowledgement (R-ACK). CRs around the sender also update their channel preference list.

Fig. 2(a), depicts all stages of MMAC-CR for four CRs $A$-$D$ and three channels $f_1$-$f_3$. During the spectrum sensing phase, CRs $A$-$D$ determine that $f_2$ is occupied by a PU. In the spectrum information sharing phase, CRs transmit a busy tone in slot 2 to indicate that $f_2$ is occupied. In the channel negotiation phase, CR $B$ performs a channel negotiation with destination $D$ and selects $f_1$ for the upcoming data phase. Similarly, pair $A$-$C$ selects $f_3$. During the data phase, pairs $B$-$D$ and $A$-$C$ switch to their selected channels to exchange data. Because a PU may appear at any channel during the data phase, the latter incorporates a periodic quiet period (QP) during which CRs perform in-band sensing. If a PU is detected, CRs abandon the current channel by switching to a back-up one.

### *B. Dedicated Control Channel CR MAC Protocols*

In a dedicated control channel design, CRs are continuously tuned to an out-of-band control channel [3], [4]. As a result, CRs must be equipped with at least two transceivers, one of which is dedicated to the control channel. As illustrated in Fig. 2(b), spectrum sensing, sharing, and channel negotiations are performed over the dedicated control channel, while data transmissions take place over the data channels. These functions are performed in a manner similar to a split-phase design with the exception of executing the control and data phases in parallel rather than sequentially.

In [3], the channel negotiation phase culminates to a single CR gaining access on the entire idle portion of the spectrum. Idle channels are merged using bonding/aggregating technology. In DOSS, data channels occupied by CRs are indicated by continuously transmitting a busy tone on a corresponding narrowband channel [4]. Any CR detecting a busy tone on a given busy tone channel will defer from transmission on the corresponding data channel.

### *C. Frequency Hopping CR MAC Protocols*

In frequency hopping (FH) CR MAC protocols, CRs hop between the available channels according to predefined FH sequences (e.g. [5]). These sequences are unique for every CR, but guaranteed to have a minimum degree of overlap (known as rendezvous). Once two CRs rendezvous on a given channel, they can exchange data or agree to synchronously hop for the duration of the data transmission. CRs skip channels that are occupied by PUs to prevent interference with PU transmissions. FH CR MAC protocols differ from their split-phase and dedicated control channel counterparts in that channel negotiations are not performed in a distributed manner, but rather follow a deterministic design.

## III. CR MAC Vulnerabilities

In this section, we detail possible CR MAC vulnerabilities due to malicious or selfish behavior from CR nodes. Such nodes violate the protocol specifications to obtain access to a larger portion of the available spectrum (selfish) or deny spectrum access to other users (malicious).

### A. Spectrum Sensing Vulnerabilities

**Distortion of Spectrum Availability:** CR MAC protocols rely on cooperative sensing mechanisms to determine the set of idle channels. A malicious CR can report false sensing observations to distort the spectrum availability. False information is particularly harmful when an "AND" rule is used to combine sensing observations. In this case, a single false report can prevent access to idle channels.

Spectrum distortion can be easily achieved in spectrum information sharing techniques that utilize busy tones [1], [4]. Such tones are unauthenticated and could be transmitted by any CR without reflecting the true channel state. As an example, referring to Fig. 2(a), malicious CR $D$ could transmit a busy tone on every slot during the spectrum information sharing phase, thus indicating that channels $f_1$-$f_3$ are occupied by PUs. CRs $A$, $B$, and $C$ will defer from communicating in the upcoming data phase. A similar attack can be mounted when the set of idle channels is reported via explicit messaging.

**Primary User Emulation (PUE) Attacks:** In a PUE attack, malicious CRs emulate the transmission characteristics of a PUs to distort the spectrum sensing process. This attack is possible because the signals transmitted by a PU are detected using signal detection techniques that do not provide any form of authentication [6]. Using the software defined radio engine, a CR can emulate PU signals that conform to the characteristics of the detectors. Referring to Fig. 2(a), malicious CR $D$ emitting emulated PU signals during the spectrum sensing phase could lead CRs $A$, $B$, and $C$ in reporting the presence of an incumbent signal on all three channels during the spectrum information sharing phase. As a result, $A$, $B$, and $C$ defer from transmiting during the upcoming data phase.

### B. Attacks on the Channel Negotiation Process

**Backoff Manipulation Attacks (BMA):** In split-phase and dedicated control channel CR MAC protocols, CRs engage in a channel negotiation process for coordinating access to the set of idle channels [1]–[4], [7]. This negotiation is contention-based, following variants of the CSMA/CA protocol. Malicious nodes that manipulate the contention protocol parameters can gain exclusive and/or more frequent access to a subset of available channels, thus occupying a disanalogous portion of the available spectrum. This can be achieved by manipulating the backoff mechanism of CSMA/CA.

In a BMA, a selfish node systematically selects small backoff values to increase its chances of reserving an idle channel compared to protocol-compliant nodes [8]. This attack is particularly effective when the control channel becomes saturated due to the large number of contending CRs, or the entire idle spectrum is assigned to a single CR [3]. In this case, CRs unable to complete a channel negotiation during the control phase, defer from transmission during the upcoming data phase.

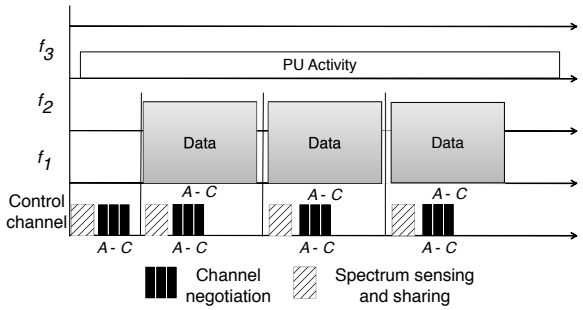


Fig. 3. Backoff manipulation attack for the CR MAC in [3]. Misbehaving CR $A$ systematically selects small backoff values during the channel negotiation phase. All idle spectrum is bonded as one channel and assigned to the $A$-$C$ communicating pair.

We use Fig. 3 to highlight the severity of a BMA. In this scenario, CR $A$ selects a small backoff value in order to seize the control channel before any other CR. Because the entire spectrum is bonded and allocated to a single CR, CRs $B$ and $D$ are deprived of channel access. Similar illustrations can be shown for other CR MAC protocols relying on CSMA/CA for control channel contention.

**Multi-Reservation Attacks (MRA):** Channel selection during the channel negotiation process is based on the expected traffic load on each of the available channels. This selection is facilitated by overhearing control messages, as various CR pairs negotiate their channel assignments. In the channel negotiation, the communicating CRs select the idle channel with the least number of reservations. At the same time, nearby CRs lower the priority of the selected channel. However, this strategy creates the opportunity for launching an MRA. In this attack, a malicious CR places multiple reservations for one or several targeted channels to lower their priority in the channel preference lists of contending CRs. As a result, protocol-compliant CRs defer from selecting the targeted channels, thus providing exclusive use of those channels to the malicious CR.

Multiple reservations on a targeted channel $f_i$ placed by a malicious CR $A$ can appear to be protocol-compiant by taking advantage of the hidden terminal problem. The malicious CR could appear to be engaged in several channel negotiations with fictitious CRs. CR $A$ broadcasts fabricated CTS messages that reserve $f_i$. The fabricated CTSs are transmitted in response to RTSs originating from fictitious CRs. Because the RTS messages are not received by any other CR in the vicinity of $A$ (these messages are never actually transmitted), CRs overhearing $A$'s CTSs consider the fictitious CRs to be hidden terminals. The reservations placed on channel $f_i$ lower the priority of $f_i$ on the channel preference lists of contending CRs.

Fig. 4 illustrates an MRA for a split-phase CR MAC protocol. In this example, six CRs are assumed to contend for idle channels $f_1$ and $f_2$. CRs $A$, $B$, and $C$ want to communicate with CRs $D$, $E$, and $F$, respectively. Malicious CR $A$ wants to reserve channel $f_2$ for exclusive use in its communication with $D$. Initially, the channel preference for $f_1$ and $f_2$ is set to zero for all CRs. CR $A$ completes one negotiation with CR

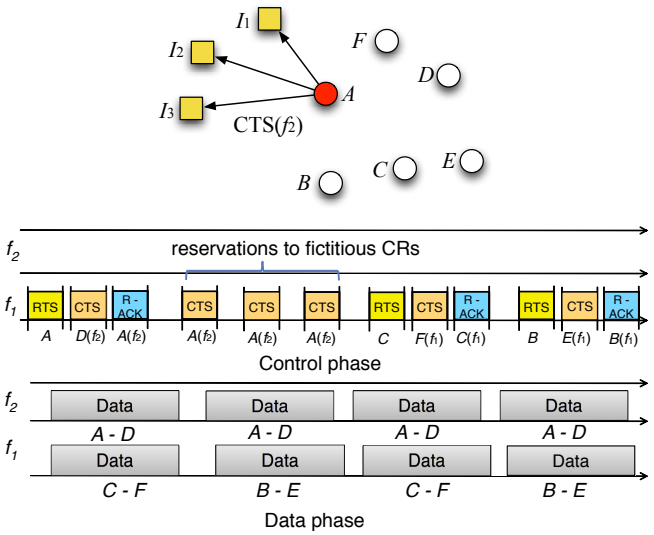


Fig. 4. CR $A$ makes four reservations on $f_2$, by completing one negotiation with $D$ and sending three CTS packets to fictitious CRs $I_1$, $I_2$, and $I_3$. All channel negotiations indicate $f_2$ as the preferred channel. CRs $I_1$, $I_2$, and $I_3$ are presumed to be hidden terminals to CRs $B$-$F$. CRs $B$-$F$ select channel $f_1$ for their data communication.

$D$ reserving channel $f_2$, thus lowering the priority of $f_2$ to -1, for CRs $B$, $C$, $E$, and $F$. To ensure that no other CR prefers $f_2$, CR $A$ broadcasts three additional CTS packets as a response to fictitious reservation requests (RTS) from fictitious CRs $I_1$, $I_2$, and $I_3$. All CTS packets from $A$ indicate $f_2$ as the preferred channel. As a result, $B$, $C$, $E$, and $F$ lower the priority of $f_2$ to -4. When pairs $B$-$E$ and $C$-$F$ perform their channel negotiations, they prefer $f_1$ since it has a higher priority than $f_2$. During the data phase, malicious CR $A$ monopolizes $f_2$ while the rest of the CRs contend on $f_1$. For a successful MRA, $A$ should place its reservations before other CRs negotiate their assignments. This can be achieved by combining the MRA with a BMA, where $A$ systematically chooses small backoff values to capture the control channel.

### C. Control Channel Denial of Service Attacks

Split-phase and dedicated control channel CR MAC designs rely on a default control channel for sharing spectrum information and coordinating access to the idle spectrum. However, the control channel constitutes a single point of failure. Launching a denial-of-service (DoS) attack on the control channel would prevent the completion of channel negotiations and ultimately the exchange of data between the CRs.

**Control channel saturation:** In split-phase CR MAC protocols, the control phase has a limited time duration. Any CRs that are unable to complete their negotiations during the control phase, defer from transmission in the upcoming data phase. This scenario occurs naturally when the control channel becomes saturated due to the large number of contending CRs. A malicious CR can intentionally saturate the control channel by broadcasting a large number of packets when not involved in channel negotiations. To reduce the risk of detection, the malicious CR can intelligently select different types of control packets to make them appear as legitimate channel negotiations. This attack could be combined with a BMA to ensure that the malicious CR captures the control channel before other CRs.

**Control channel jamming:** A malicious CR can also selectively jam control packets during the channel negotiation phase. For most CR MAC protocols, channel negotiations involve a three-way handshake consisting of an RTS, CTS, and R-ACK exchange. The timing between the transmission of these three messages is fixed and known to all CRs. A malicious CR overhearing the transmission of an RTS (CTS) can jam the corresponding CTS (R-ACK), thus preventing the completion of the channel negotiation. Here, we emphasize that control packets are typically encoded with limited error correction capabilities. Hence, jamming a small number of symbols is sufficient to prevent packet decoding at the receiver.

CR MAC protocols relying on FH are less vulnerable to jamming since they asynchronously hop to the set of idle channels [5]. Here, a jamming CR in knowledge of the FH sequence $h_i$ of a targeted CR can launch a DoS on that CR by following $h_i$. However, the impact of this attack is limited since other CRs are free to communicate on other channels.

## IV. Countermeasures

### A. Countering Attacks on Spectrum Sensing

**Countering Distortion of Spectrum Availability:** Cooperative sensing is vulnerable to spectrum availability distortion attacks due to the conservative nature of the hard decision combining mechanism. To avoid interference with PUs, channel availability is determined by following an "AND" rule. A channel is considered to be free of PU activity if all cooperating CRs agree on its idle state. A single report from a malicious CR is sufficient to discard an idle channel from further use.

To mitigate the impact of such attacks, decision combining mechanisms using *threshold voting* rules can be employed. In threshold voting, a channel is deemed to be occupied by a PU, if at least $\tau$ out of $n$ CRs report it to be busy, where $\tau$ is a system-defined parameter. Under threshold voting, a small number of colluding CRs cannot distort the spectrum availability. The caveat of a threshold rule is that it does not always account for the spatial variations of PU activity. As an example, an occupied channel detected by a small number of CRs could be falsely declared as idle. To alleviate this drawback, parameter $\tau$ must be adaptive to the spacial variations of PU activity.

Threshold voting is easily implemented when spectrum information sharing is realized via the exchange of authenticated messages. However, several CR MAC protocols employ simpler forms of information sharing such as busy tones [3], [4]. Busy tones are not authenticated, nor do they account for the number of CRs reporting on the channel state. One candidate solution could be the measurement of the busy tone power. If multiple CRs transmit a busy tone on the corresponding slot, the power of that tone is expected to be high. However, a malicious CR may intentionally increase the power of its busy tone to defeat a power-based busy tone threshold voting technique.

**Countering Primary User Emulation Attacks:** Even if threshold voting is selected as the cooperation rule, the spectrum availability can still be distorted under a PUE attack.

When a malicious CR emulates PU activity on a channel $f_i$, all nearby CRs detect $f_i$ to be busy. Hence, $f_i$ is declared to be busy under either an "AND" or a threshold voting rule. Defending against a PUE attack is challenging because the energy or feature detectors used during spectrum sensing cannot verify the authenticity of a PU signal. Moreover, current regulations prohibit any modifications on legacy systems.

Several mechanisms have been proposed for authenticating PU activity without imposing any modifications on the PU network. If the locations of PUs are known a priori, PU signals can be authenticated by determining the position of the PU transmitter [9]. This can be achieved by estimating the distance between the PU and several receiving CRs using the received signal strength (RSS) and computing the PU location using trilateration. Manipulation of the transmission power by a malicious CR for emulating the fixed PU position becomes challenging if the malicious CR is not within less than a few meters from the legitimate PU. PU signal authentication can also be achieved by constructing an RF signature of the PU-CR channel [10], [11]. RF signatures capture unique characteristics of the RF channel (channel and frequency response) between two stationary nodes, based on random multipath components. These characteristics cannot be emulated unless the malicious CR is located within a few wavelengths from the emulated PU. Assuming that PU nodes are physically protected, mounting a PUE attack that emulates the RF channel becomes challenging.

### *B. Countering Attacks on the Control Channel*

**Countering Backoff Manipulation Attacks:** BMA attacks are mitigated by regulating and monitoring the backoff schedule of contending nodes. In [8], the backoff value of a sender is assigned by the corresponding receiver. The receiver is responsible of monitoring the sender's compliance with the assigned backoff value. If the sender deviates from that value, the receiver "punishes" the sender by assigning larger backoff values for future transmissions. Repeated violations lead to the characterization of the violating node as misbehaving, and eventually to its removal from the network.

The receiver-based backoff assignment mechanism is not effective when the receiver colludes with the sender. Moreover, a malicious receiver may purposefully assign large backoff values to a sender to alleviate contention for its own transmissions. To counter sender-receiver collusion, the number of CRs monitoring the backoff values of other CRs must be increased. This can be achieved by forcing every CR publish its backoff schedule ahead of time. Every CR could broadcast the unique seed of a publicly known pseudorandom number generator used for the generation of the backoff values. Neighboring CRs can then monitor the backoffs selected by their peers and detect misbehaving CRs that violate their backoff schedules.

**Countering Multi-reservation Attacks:** CR MAC protocols are vulnerable to MRAs due to: (a) the adjustment of channel priorities based on the number of reservations placed on each channel, and (b) the exploitation of the hidden terminal problem for introducing fictitious nodes. The former vulnerability can be countered by modifying the channel priority rules such that the priority of a channel $f_i$ is lowered only if new CR pairs place reservations on $f_i$. Referring to the attack scenario presented in Fig. 4, multiple reservations placed by malicious CR $A$ on channel $f_2$ would only lower the priority of $f_2$ by one. Thus, CR $A$ would not be able to isolate $f_2$ from the rest of the CRs.

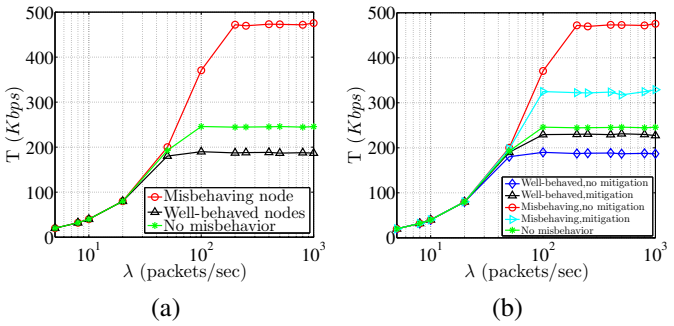


Fig. 5. (a) $T$ as a function of $\lambda$ under an MRA and BMA, (b) $T$ as a function of $\lambda$ for the misbehaving and well-behaved CRs, under the modified channel priority rules.

Communication with fictitious CRs for the purpose of placing multiple reservations can be defeated by employing secure two-hop neighbor discovery protocols. These protocols are executed during the network setup phase and are periodically repeated if the CRs are mobile. If the two-hop neighborhood is securely known, CRs are aware of the identities of all CRs that are hidden terminals. Hence, malicious CRs cannot pretend to communicate with fictitious CRs.

**Performance Evaluation:** We evaluated the impact of the BMA and the MRA and of the proposed countermeasures using the OPNET Modeler packet-level simulator. We considered a single-hop CR network of six CR pairs with opportunistic access to three orthogonal channels, capable of a 2Mbps data rate. We implemented the split-phase CR MAC protocol illustrated in Fig. 2(a). The control and data phases were fixed to 20ms and 80ms, respectively. The packet arrival process at the MAC layer was assumed to follow a Poisson distribution with parameter $\lambda$. Each data packet was set to 512 bytes. Misbehavior strategies were implemented on a single sender. The simulation lasted 40s and results were averaged over 40 runs.

Fig. 5(a) shows the average throughput $T$ achieved by the misbehaving and protocol-compliant CRs under normal operating conditions and under the combination of a BMA and an MRA. We observe that the misbehaving CR achieves almost three times the throughput of any protocol-compliant CR under traffic saturation conditions. This is because the misbehaving CR does not have to share its channel during the data phase, while protocol-compliant nodes have to contend in the remaining two channels, when PU activity is absent. Fig. 5(b) compares the average throughput of the misbehaving CR and the average per-flow throughput of protocol-compliant CRs under the modified channel priority rules and when a secure two-hop neighbor discovery protocol is applied. We observe that the adversary's throughput drops by 150Kbps while the throughput of protocol-compliant CRs increases by 40Kbps.

**Countering Control-channel DoS Attacks:** DoS-resilient control channel designs distribute the control operation in space

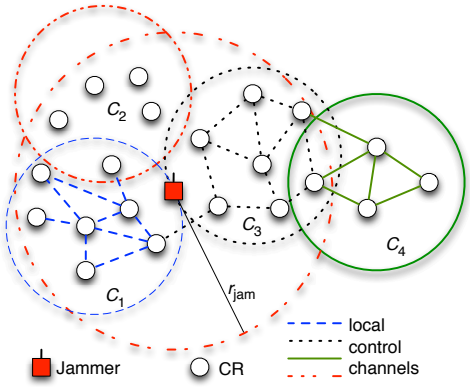


Fig. 6. A cluster-based CR network under jamming attack. Clusters $C_1$ - $C_4$ are allocated different control channels based on the local spectrum availability. A jamming attack with range $r_{jam}$ on the control channel assigned to cluster $C_2$ has limited impact on that cluster.

and frequency [2], [12]. These designs follow a cluster-based approach where the control channel is locally established at each neighborhood according to the local spectrum availability. Hence, long-range DoS attacks cannot simultaneously impact the control channel on all parts of the network. A cluster-based control channel allocation is shown in Fig. 6, where long-range jamming on cluster $C_2$ only affects communication within $C_2$.

Cluster-based approaches are still vulnerable to local jamming. Several anti-jamming techniques dynamically allocate the control channel on multiple frequency bands based on cryptographic information or FH [13]–[15]. In [13], each CR is aware of a subset of control channels according to a unique cryptographic key. Hence, a malicious CR cannot jam all control channel locations. An alternative method assigns unique FH sequences to each CR [14]. The overlap between those sequences implements the control channel. A malicious CR jamming the control channel according to its FH sequence becomes uniquely identifiable. An effective method for mitigating control channel jamming is to eliminate the need for a control channel overall. The authors of [15] proposed an FH scheme where the CR sender and receiver independently hop to the same set of idle channels with high probability. The channel selection process at the sender and the receiver is formulated as a non-stochastic multi-armed bandit (NS-MAB) problem.

## V. Research Challenges and Conclusions

Prior work on CR MAC protocol design has been primarily focused on addressing the dynamic nature of spectrum availability. Various MAC coordination algorithms coordinate channel access between multiple CRs in a fair manner and without causing interference to legacy systems. However, prior work does not consider the cases of CR misbehavior and malicious external attacks. As we showed in this article, selfish or malicious CRs can manipulate the protocol parameters in order to gain a larger share of the idle spectrum. At the same time, they can deny spectrum access to protocol-compliant CRs.

CR MAC layer vulnerabilities are partly attributed to the simplistic nature of the individual and cooperative spectrum sensing mechanisms employed for detecting the idle channels. These operations are performed in an insecure manner, without authenticating the sensed information. Securing distributed and cooperative sensing mechanisms largely remains an open and challenging problem. Moreover, the channel negotiation process for sharing the idle spectrum is vulnerable to parameter manipulation from non-compliant CRs. These vulnerabilities can be mitigated by applying behavioral monitoring techniques that identify the misbehaving nodes and isolate them from the network. The challenge here is to ensure that behavioral monitoring can be achieved in a resource-efficient manner, without degrading the overall CR network performance.

## Acknowledgments

This research was supported in part by the National Science Foundation (under grants CNS-0844111, CNS-1016943, and CNS-1145913). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF.

## References

[1] Michael Timmers, Sofie Pollin, Antoine Dejonghe, Liesbet Van der Perre, and Francky Catthoor. A distributed multichannel MAC protocol for multihop cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 59(1):446–459, 2010.

[2] Jun Zhao, Haitao Zheng, and Guang-Hua Yang. Spectrum sharing through distributed coordination in dynamic spectrum access networks. *Wireless Communications and Mobile Computing*, 7(9):1061–1075, 2007.

[3] Hang Su and Xi Zhang. Cross-layer based opportunistic MAC protocols for QoS provisionings over cognitive radio wireless networks. *IEEE Journal on Selected Areas in Communications*, 26(1):118–129, 2008.

[4] Liangping Ma, Xiaofeng Han, and Chien-Chung Shen. Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks. In *Proc. of the IEEE DySPAN Symposium*, pages 203–213, 2005.

[5] Kaigui Bian and Jung-Min Park. Asynchronous channel hopping for establishing rendezvous in cognitive radio networks. In *Proceedings of the IEEE INFOCOM Conference*, pages 236–240, 2011.

[6] Ruiliang Chen, Jung-Min Park, Y. Thomas Hou, and Jeffrey H. Reed. Toward secure distributed spectrum sensing in cognitive radio networks. *IEEE Communications Magazine*, 46(4):50–55, 2008.

[7] Hang Su and Xi Zhang. CREAM-MAC: An efficient cognitive radio-enabled multi-channel mac protocol for wireless networks. In *Proceedings of the IEEE WoWMoM Symposium*, pages 1–8, 2008.

[8] Pradeep Kyasanur and Nitin H. Vaidya. Selfish MAC layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing*, 4(5):502–516, 2005.

[9] Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, 2008.

[10] Yao Liu, Peng Ning, and Huaiyu Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *Proceedings of the IEEE S&P Symposium*, pages 286–301, 2010.

[11] Swathi Chandrashekar and Loukas Lazos. A primary user authentication system for mobile cognitive radio networks. In *Proceedings of the ISABEL Symposium*, pages 1–5, 2010.

[12] Sisi Liu, Loukas Lazos, and Marwan Krunz. Cluster-based control channel allocation in opportunistic cognitive radio networks. *IEEE Transactions on Mobile Computing*, 11(10):1436–1449, 2012.

[13] Patrick Tague, Mingyan Li, and Radha Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In *Proceedings of the PIMRC Symposium*, pages 1–5, 2007.

[14] Sisi Liu, Loukas Lazos, and Marwan Krunz. Thwarting control-channel jamming attacks from inside jammers. *IEEE Transactions on Mobile Computing*, 11(9):1545–1558, 2012.

[15] Qian Wang, Kui Ren, and Peng Ning. Anti-jamming communication in cognitive radio networks with unknown channel statistics. In *Proceedings of the IEEE ICNP Conference*, pages 393–402, 2011.