MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks

Kaigui Bian and Jung-Min Park
ARIAS (Advanced Research in Information Assurance and Security) Lab
Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
{kgbian, jungmin}@vt.edu

***Abstract*—The Federal Communication Commission (FCC) regulates radio spectrum by applying regulatory paradigms. In the conventional spectrum management paradigm, a group of primary users is given license to operate exclusively in a specific band. Recent studies have shown that a new paradigm is needed to alleviate the spectrum shortage problem. In the new paradigm, licensed bands are opened up to unlicensed operations by secondary users on a non-interference basis to primary users. Cognitive radio (CR) technology is seen as the enabling technology for realizing this new paradigm. Emergency communication networks and military tactical networks of the future are expected to be built from multi-hop CR networks. In a typical MAC protocol designed for multi-hop CR networks, a node uses the common control channel to perform channel negotiations before data transmission. Recent research findings indicate that the common control channel is highly vulnerable to network attacks. In this paper, we examine MAC layer misbehaviors in multi-hop (ad-hoc) CR networks. First, we study the problem of control channel saturation attacks. This type of attack can cripple the channel assignment process. Second, we investigate selfish misbehaviors that exploit deficiencies in MAC protocols for CR networks. We use simulation data to evaluate the impact of such misbehaviors in terms of network availability and fairness.**

***Index Terms*—MAC protocol, network security, cognitive radio, channel negotiation, multi-hop networks**

I. INTRODUCTION

Cognitive radio is seen as an enabling technology for a new spectrum utilization paradigm called opportunistic spectrum sharing (OSS). In this paradigm, *unlicensed users* (a.k.a. *secondary users*) equipped with CRs "opportunistically" operate in fallow licensed spectrum bands without causing interference to *licensed users* (a.k.a. *primary* or *incumbent users*) [1]. In CR networks, distributed *spectrum sensing* is employed to identify fallow spectrum bands and map them into several logical channels [2]. Information gathered from spectrum sensing is used by a dynamic spectrum allocation (channel assignment) mechanism [3] to allocate free channels among contending CR nodes. In multi-hop (ad-hoc) CR networks[1], secondary users need to exchange local spectrum sensing and channel assignment information for the network to carry out distributed spectrum sensing and channel assignment processes. In most of the MAC protocols proposed for CR networks (e.g., [3, 4, 5]), the *common control channel* plays a key role in enabling the nodes to exchange local information.

Like conventional wireless networks, CR networks are vulnerable to attacks unless security mechanisms are implemented in sufficiently robust form. In a single-hop CR network (e.g., IEEE 802.22 [2] [6]), confidentiality and authentication across the network can be provided by applying cryptographic transforms to the MAC frames. For example, a *security sublayer* is implemented in IEEE 802.22 to provide its subscribers with certain security assurances. The security sublayer employs an authenticated client/server key management protocol. Unfortunately, such a protocol cannot be implemented in a multi-hop CR network, where there is no trusted entity to act as a server to control distribution of keying material. Hence, providing security assurance in a multi-hop network is a greater challenge.

Adversaries can cause significant harm by exploiting the vulnerabilities of a multi-hop CR MAC. For instance, without an authentication mechanism, it is feasible for adversaries to forge MAC frames or insert spurious information in the MAC control frames to cause communication disruptions or gain an unfair advantage in resource allocation.

In this paper, we identify vulnerabilities shared by most of the MAC protocols proposed for multi-hop CR networks. Then, we describe attacks that can exploit these vulnerabilities. Specifically, we investigate two types of MAC layer misbehaviors: Denial-of-Service (DoS) attacks and selfish misbehaviors. In the first type of misbehavior, an adversary cripples the common control channel by exploiting the *control channel saturation* problem [7]. Such an attack can cripple the various control functions performed by the control channel, especially the dynamic resource allocation function. In the

The work presented in this paper was supported in part by the National Science Foundation under Grant CNS-0524052.

[1] Throughout the paper, we use the term multi-hop CR network to denote multi-hop ad hoc CR networks.

[2] IEEE 802.22 is the first worldwide wireless standard based on cognitive radio technology. It specifies the air interface for wireless regional area networks that access fallow TV spectrum.

selfish misbehavior problem, a selfish CR node disrupts the packet forwarding process by acting dishonestly in the *channel negotiation* process. We investigate the impact of the aforementioned attacks via simulation results. Then, we briefly discuss potential countermeasures against such MAC layer misbehaviors.

The rest of the paper is organized as follows. Related work is presented in Section II, and technical background on multi-hop CR networks is given in Section III. We describe DoS attacks in multi-hop CR networks in Section IV, and give details on MAC-layer selfish misbehaviors in Section V. Possible countermeasures against such MAC layer misbehaviors are discussed in Section VI. We conclude the paper in section VII.

II. Related Work

MAC-layer misbehaviors have been studied previously in the context of 802.11 DCF (Distributed Coordination Function) [8]. We discuss some of these misbehaviors here, since they share some traits in common with MAC-layer misbehaviors in CR networks. Misbehaviors in the context of 802.11 DCF can be classified into two categories: malicious misbehaviors and selfish misbehaviors [9]. The primary aim of a host carrying out malicious misbehaviors is to disrupt normal network operations, which does not necessarily lead to the performance gain of the misbehaving host. Malicious misbehaviors include routing disruption attacks and jamming attacks. In contrast, selfish hosts misbehave primarily to improve their own performance (throughput, latency, energy dissipation rate, etc.).

DoS attacks at the MAC layer are a significant threat to the availability of network services. An adversary's objective in launching a DoS attack is to prevent or hamper non-malicious nodes from accessing the channel. For instance, in [10], the authors study simple DoS attacks at the MAC layer, and show simulation results for different attack traffic patterns. In [11], the authors describe vulnerabilities in the 802.11 MAC protocol and show how to exploit them by tampering with the firmware. In [12], Raya et al. discuss MAC layer misbehaviors in wireless hotspots. The authors describe a type of misbehavior in which an adversary sends RTS/CTS frames to spuriously reserve the channel without any intention of actual data transmissions. The paper also discussed detection techniques for detecting such attacks.

A selfish host misbehaves in order to gain an unfair advantage in terms of channel access. In 802.11 DCF, a selfish host unilaterally modifies parameters in the back-off mechanism to get priority access to the channel. As a result, the selfish node achieves better throughput. Kyasanur and Vaidya [9] proposed a detection scheme and a correction mechanism for thwarting one type of MAC layer selfish misbehavior. Their main idea is to let the receiver assign and send back-off values to the sender in CTS and ACK frames and then use those values later to detect misbehavior. The correction scheme adds a penalty in the next back-off time if selfish misbehaviors are detected. Cagalj et al. [13] studied selfish misbehaviors at the MAC layer using a game-theoretic framework. Using a dynamic game model, the authors were able to derive a strategy that each node should follow for the network to reach equilibrium. In the model, each node controls its channel access probability by adjusting the size of its contention window. The model is valid under the assumption that all nodes are within range of each other.

III. Technical Background

In this section, we provide some technical background related to the MAC layer of a multi-hop CR network. Since there is no existing standard that defines such a MAC layer, the discussions given here are based on the common features shared by most of the multi-hop CR MAC protocols that were proposed recently.

A. Distributed Channel Negotiation in Multi-hop CR MAC

In a typical multi-hop CR network, nodes contend for channels by exchanging MAC control frames in the common control channel [3]. Since there is no access point or base station, channel negotiation is carried out in a distributed manner, between each pair of transmitter and the intended receiver [3, 5, 14]. During channel negotiations, the following types of MAC frames are utilized: Free Channel List (FCL), SELection (SEL), and REServation (RES).

Fig. 1 shows a simple example of a channel negotiation process between a sender and a receiver. Here, the "sender" is the host that transmits the MAC data frames, and the "receiver" is the host that receives the MAC data frames. The sender first identifies fallow spectrum bands and maps them into logical channels. Then it obtains a free channel list (FCL frame) and sends this to the receiver after waiting a random *back-off* time. Upon receiving the FCL, the receiver identifies available data channels common to both sides, and then selects one data channel according to a data channel selection policy. The channel selection is indicated in a SEL frame and sent back to the sender. After receiving the SEL frame, the sender notifies its neighbors of the channel selection via a channel reservation message (RES frame). Both neighbor 1 and

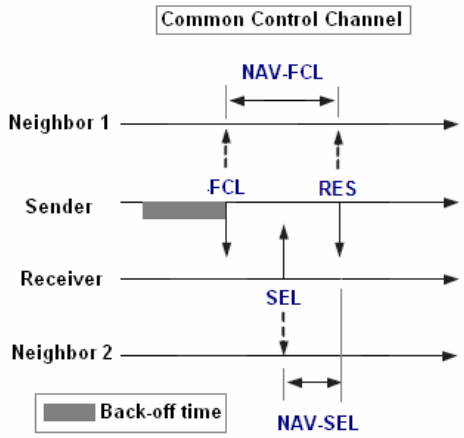

Fig. 1. Distributed channel negotiation process between a sender and a receiver.

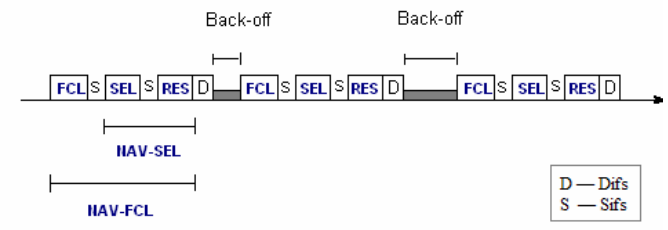

Fig. 2. The sequence of MAC control frames (FCL-SEL-RES sequence) in the control channel. The time interval "D" denotes Distributed inter frame space (Difs), and the time interval "S" denotes Short inter frame space (Sifs).

neighbor 2 refrain from transmitting by maintaining a network allocation vector (NAV) specified in the FCL and SEL frames overheard during the channel negotiation process. From the perspective of the control channel, a sequence of MAC control frames (FCL-SEL-RES sequence) is exchanged for each channel negotiation process, as shown in Fig. 2. Using the above process, a sender and a receiver selects a data channel for communicating.

B. Control Channel Hopping in Multi-hop CR MAC

As aforementioned, the common control channel plays a key role in performing various control mechanisms in multi-hop CR networks [3]. For instance, secondary users use the common control channel to send local sensing reports to a fusion center during cooperative spectrum sensing [2, 3]. In addition, the exchange of MAC frames during channel negotiations is carried out in the common control channel as described previously.

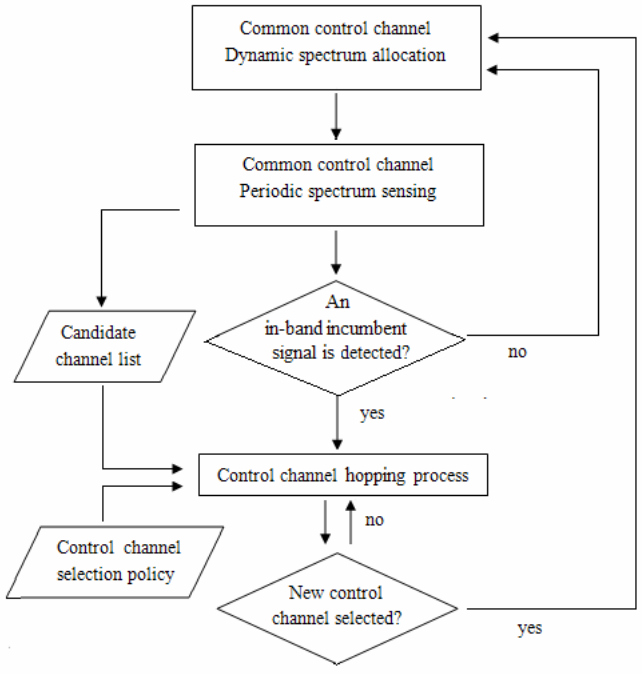

Fig. 3. A flowchart of the control channel hopping process.

In a CR network that is utilizing licensed spectrum, a given link's channel may be interrupted at any time by the appearance of incumbent signals [3, 4, 5, 15]. When an incumbent (or primary) signal is detected in a channel, secondary users need to vacate the channel and switch (or "hop") onto another channel to resume transmissions. Even the control channel needs to switch to another band if the presence of an incumbent signal is detected in its current band. Therefore, a control channel hopping mechanism is necessary in CR networks.

When an incumbent signal is detected in the same band as the current control channel, a replacement is selected from a candidate control channel list. The candidate control channel list is maintained proactively during distributed spectrum sensing [6]. A control channel selection policy [3, 6] is applied when selecting a new control channel from the list. A flowchart of the control channel hopping process is illustrated in Fig. 3.

IV. Denial of Service Attacks

In this section, we describe how an adversary can exploit the vulnerabilities of a multi-hop CR network's MAC layer to launch a DoS attack against it.

A. Network Assumptions

Adhering to a predefined control channel selection policy, we assume that secondary users select a replacement channel from the candidate channel list when an incumbent signal is detected in the same band as the current common control channel.

We also assume that each CR node is equipped with two radios, one for the control channel and the other one for data channels. The control radio is fixed on the common control channel and the data radio can be switched for either transmitting or receiving traffic on a data channel.

B. Vulnerabilities of Multi-hop CR MAC Protocols

Based on the analysis of recently proposed MAC protocols for multi-hop CR networks, we concluded that these protocols share the following vulnerabilities.

1) Lack of MAC Layer Authentication

In an 802.22 WRAN (wireless regional area network), which is a single hop network, there is a security sublayer that provides confidentiality and authentication of MAC frames. The security sublayer thwarts MAC-layer DoS attacks by preventing the modification or forgery of MAC frames. The security sublayer employs an authenticated client/server key management protocol in which the base station acts as the trusted server. Unfortunately, such a protocol cannot be implemented in a multi-hop CR network since there is no trusted entity to act as a server to control distribution of keying material. Without an authentication mechanism, adversaries can forge MAC control frames to launch DoS attacks.

2) Control Channel Saturation Problem

In a multi-channel environment, such as the MAC-layer of a CR network, the control channel can become a bottleneck for network performance. High traffic load in the network may

cause frequent exchanges of control packets, which saturates the control channel. Moreover, control packet collisions lead to low efficiency of all control mechanisms, including channel negotiation.

From the perspective of security, the control channel plays a key role in network availability. If attackers can successfully saturate the control channel, they can severely obstruct the channel negotiation and allocation process, thus causing denial of service. In a multi-hop CR MAC protocol, an adversary can readily forge channel negotiation frames to launch a DoS attack. Such spurious MAC frames can saturate the control channel so that legitimate users cannot utilize their share of the control channel to negotiate and assign data channels.

3) Predictable Control Channel Hopping Sequence

If control frames are exchanged in unencrypted form (i.e., as plaintext), the candidate channel list can be readily acquired by any secondary user, including an adversary. With the candidate channel list, an attacker can easily predict the next control channel in the hopping sequence. This capability enables the attacker to continually saturate the control channel, even if the control channel continuously hops among different bands due to the presence of incumbent signals.

C. DoS Attack Model

We describe an attack that saturates the common control channel of a multi-hop CR MAC to cause denial of service. In the attack, an adversary saturates the control channel by transmitting spurious MAC control frames, thus obstructing data flows traversing within its transmission range. The distinguishing features of the attack include: (1) the attack is difficult to detect because the adversary uses certain types of control frames whose spuriousness cannot be readily detected; and (2) the cost associated with launching the attack is small since a relatively small number of spurious control frames need to be transmitted by the attacker for the attack to be effective.

1) Attack Goal

The goal of the attacker is to cause denial of service to a given network by saturating the common control channel.

2) Attack Method

The adversary's attack method is straightforward: send a sufficient number of spurious control frames to saturate the control channel.

To minimize the chance of detection, an adversary may opt use only certain types of control frames in its attack. We argue that the chance of detection can be reduced if the attack is carried out with FCL and SEL frames and not with RES frames. The justification for this argument is given in the following paragraphs.

Recall that an FCL frame includes a list of free channels as recognized by a sender. An FCL frame also contains a NAV value that reserves the control channel until the end of the current channel negotiation process. When a malicious node transmits spurious FCL frames, it is difficult for neighboring nodes to detect whether the frames are spurious because the information contained in them cannot be checked for legitimacy. Specifically, there is no way to check the legitimacy of the list of free channels and the NAV value.

Recall that a receiver sends an SEL frame to the sender in response to receiving an FCL frame sent by the sender. The legitimacy of an SEL frame can be checked by verifying whether the sender transmits in the channel specified in the SEL frame. Therefore, spurious SEL frames can be detected only by nodes that are within range of both the sender and the receiver. This makes detection more difficult.

Recall that a RES frame transmitted by the sender to the receiver indicates the data channel selected for data transmission. Any node within the sender's range can readily verify the RES frame's legitimacy by checking whether the sender actually uses the channel indicated in the RES frame in its data transmissions.

We conclude that an attacker can reduce the chance of being detected by utilizing spurious FCL and SEL frames and not RES frames.

D. Simulation Results

We assume that channel negotiation is carried out in a common control channel. It is assumed that packets are transmitted immediately after a data channel has been allocated via channel negotiation. In the simulation experiments, we set the control channel capacity as 2Mb/s, and used TCP Reno as the transport-layer protocol.

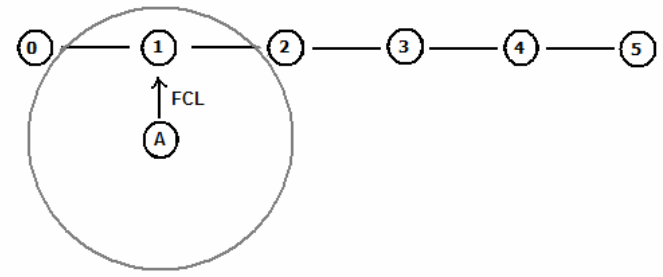

Fig. 4. Illustration of the "chain" network topology.

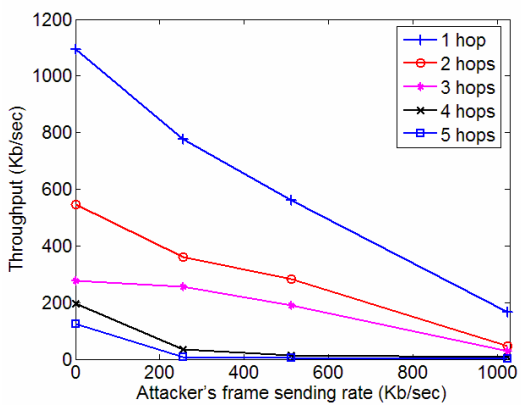

Fig. 5. Throughput vs. attacker's sending rate in the "chain" topology.

In the first scenario that we considered, a simple "chain" network topology was assumed as shown in Fig. 4. The node labeled with "A" is the attacker node, and the circle encompassing the attacker node represents its transmission

range. We assume that the attacker node transmits spurious control frames according to a Poisson process. Node 0 is always the source node and the destination node can be any one of the other nodes, labeled 1 through 5. The simulation results are shown in Fig. 5. As expected, the end-to-end throughput dropped sharply as the attacker's sending rate increased. Results indicate that the attack's impact on a flow varies depending on the length (i.e., number of hops) of that flow.

In the next set of simulation experiments, we investigated the attack's impact in more realistic network topologies, using a greater number of nodes.

1) Network Model

We considered a network with 50 CR nodes distributed randomly in a 1600m×1600m square area. In addition to those 50 legitimate nodes, there are 20 malicious nodes in the network. The transmission range of each node is 250m. Each legitimate node randomly creates a TCP flow to a randomly chosen destination, while each attacker only sends FCL frames. We observed the impact of this attack using two metrics: end-to-end throughput and delay. We carried out the simulation experiments under different scenarios by changing the following parameters: percentage of attacker nodes, mobility, and network traffic load. Each result is the average value of 10 simulation runs.

2) Stationary Nodes

The simulation results obtained using the aforementioned network model are illustrated in Figs. 6 and 7. All nodes are assumed to be stationary. In Fig. 6, the average end-to-end throughput as a function of the percentage of attackers is plotted. We can clearly see that the throughputs of the multi-hop flows are severely throttled by the attack. The attack makes it very difficult for intermediate nodes of a multi-hop path that are within transmission range of an attacker to forward data packets since the control channel is saturated with attack frames.

In Fig. 7, we plotted the average end-to-end delay versus the percentage of attackers. For paths longer than two hops, the value of the end-to-end delay was close to infinity because a large proportion of the packets did not reach their respective destinations.

From the above simulation results, we can conclude that the MAC-layer DoS attack brings about a *network partition* effect in terms of both end-to-end throughput and delay. That is, the attack severely degrades throughput and increases delay in multi-hop paths, thus partitioning a given network into many isolated regions in which inter-region traversal of packets is restricted. This phenomena is more prevalent in longer flows.

3) Mobile Nodes

To investigate the relation between nodes' mobility and the attack's effectiveness, we observed the average end-to-end throughput in four different scenarios. These scenarios are: (1) static legitimate nodes and static attacker nodes, (2) static legitimate nodes and mobile attacker nodes, (3) mobile legitimate nodes and static attacker nodes, and (4) mobile legitimate nodes and mobile attacker nodes. The results are shown in Fig. 8. The results indicate that the mobility of the attackers have very little impact on the end-to-end throughput of the flows within the network. On the other hand, the mobility of the legitimate nodes did have an impact on their flows' throughput as expected.

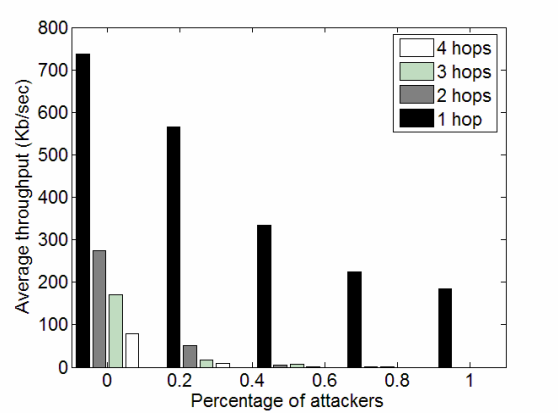

Fig. 6. Average end-to-end throughput vs. percentage of attackers in a malicious network scenario.

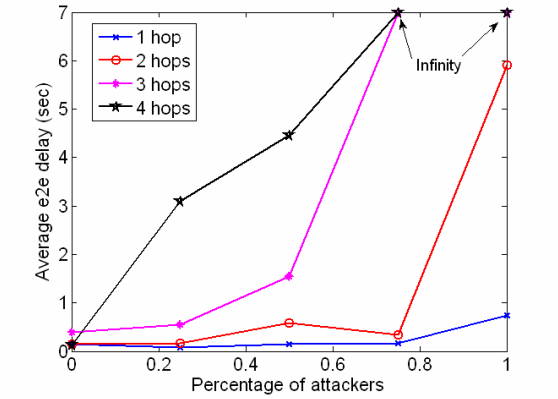

Fig. 7. Average end-to-end delay vs. percentage of attackers in a malicious network scenario.

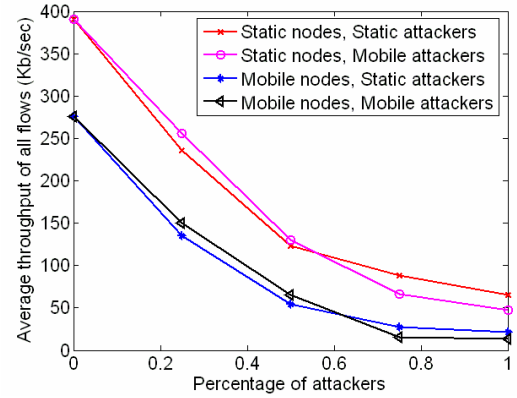

Fig. 8. Average throughput in static and mobile network scenarios.

4) Network Traffic Load

We investigated the impact of the DoS attack in two

different network traffic load conditions: one with 5 TCP flows and the other with 10 TCP flows. Results are shown in Fig. 9. As expected, the effect of the attack was more evident when the network was under the lighter traffic load. When the network was under the heavier traffic load, the effect of the attack was less evident since the flow's average throughput was already degraded by the increased traffic.

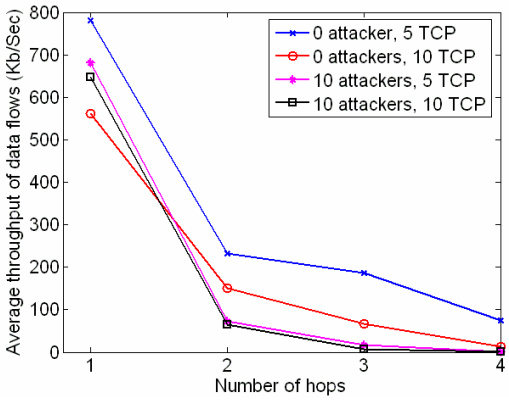

Fig. 9. Average throughput under different traffic load scenarios.

V. Selfish Misbehaviors

In this section, we investigate on another type of MAC-layer misbehavior, which was call *selfish misbehaviors*. Specifically, we focus on a type of misbehavior in which a node acts selfishly during a channel negotiation process for its own benefit.

A. Selfish Channel Negotiation

Misbehaviors by a selfish node include a diverse range of demeanors that degrades a network's overall performance. An adversarial node's motive for carrying out selfish misbehaviors is to gain an unfair advantage in terms of maximizing channel usage and minimizing its energy dissipation [9]. In other words, a selfish host in a network would try to improve its own performance (such as throughput, end-to-end delay, etc.) at the cost of the network's overall performance. As a result, the performance of the network and network fairness will deteriorate.

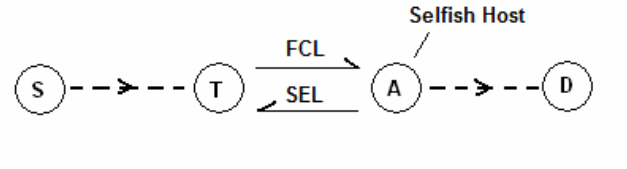

Fig. 10. An illustration of the channel negotiation process between node T and the selfish node.

At the MAC layer of a multi-hop CR network, distributed channel negotiation is performed using the results obtained from spectrum sensing. The fairness of channel assignments depends on the cooperation of contending nodes. However, the cooperation of nodes in a multi-hop network cannot be assured or enforced. In a distributed channel negotiation scheme, a selfish node can readily conceal available data channels from others and reserve them for its own use by refusing to forward data packets from an upstream node. An example is shown in Fig. 10. In the figure, node A is a selfish node. Suppose that the selfish node was chosen as an intermediate node on a routing path from node S to node D. After receiving an FCL frame from node T, node A replies with a fraudulent SEL frame indicating that no free channels are available. Node T cannot verify the legitimacy of this SEL frame because it cannot overhear all transmissions within the reception range of Node A.

In the above example, other nodes cannot transmit data packets via the selfish node, and the selfish node can monopolize the local spectrum. The benefits that node A would receive is two folds: node A can increase its own throughput and it can conserve energy by refusing to forward others' data packets.

Recent studies show that MAC-layer selfish misbehaviors can seriously degrade a conventional wireless networks' performance [9]. The same is true for CR networks. In the next section, we investigate the impact of selfish misbehaviors on network fairness.

B. Impact on Network Fairness

To measure network fairness, Jain's fairness index [16] is often used. It is defined as

$$\text{Fairness index} = \frac{\left(\sum_f R_f\right)^2}{n\sum_f R_f^2}, \quad (1)$$

where R_f is the measured throughput of each data flow and n is the total number of flows in a given network.

We conducted a simulation experiment to observe the impact of selfish misbehaviors on network fairness, using Jain's fairness index to quantify fairness. A fairness index value of one indicates a "perfectly" fair network. The results are shown in Fig. 11. The network model used in Section IV was also used here, except that a subset of the nodes carried out selfish misbehaviors instead of DoS attacks.

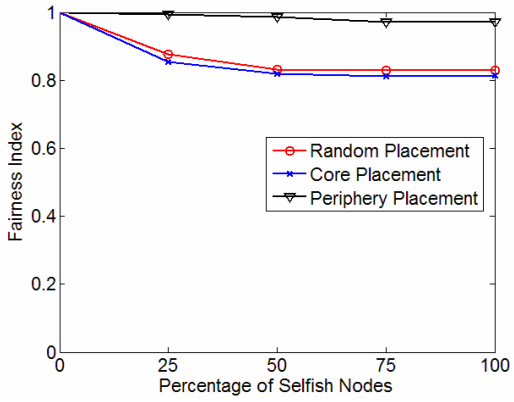

Fig. 11. System Fairness Index vs. percentage of selfish nodes.

In Fig. 11, the simulation result is plotted by calculating the value of the system fairness index in (1). The fairness index

was measured under three different scenarios, where each scenario is different in terms of the selfish node placement. Three different placement schemes were used: random placement, placement at the periphery of the network, and placement at the core of the network. The results indicate that placing selfish nodes at the periphery of the network does little to effect network fairness. This observation can be attributed to the fact that nodes at the periphery are less likely to be selected as intermediate nodes on a routing path, thus giving the nodes less opportunity to carry out selfish misbehaviors.

VI. Discussions on Countermeasures

In Sections IV and V, we have discussed two types of MAC-layer misbehaviors: DoS attacks and selfish misbehaviors. At the core of both types of misbehaviors, the transmissions of forged or fraudulent control frames are involved. These problems can be resolved, or at least alleviated, if a MAC-layer authentication scheme is employed. For instance, authenticated control frames would prevent the creation of forged control frames and aid in the traceback of nodes that transmit control frames with false information. In the IEEE 802.22 standard, a security sublayer is used to provide confidentiality and authentication at the MAC layer. According to the draft standard, the security sublayer would also provide some protection against certain types of DoS attacks. Unfortunately, implementing such a sublayer is very difficult in a multi-hop CR network because there is no trusted entity to act as a key management server. In other words, the use of cryptosystem based countermeasures may be impractical in multi-hop CR networks since such countermeasures would require a key distribution/management infrastructure.

Perhaps a more practical countermeasure is to deploy a scheme that can detect attacks and even identify the attacker nodes. Such schemes have been studied in the context of 802.11 networks [12, 17]. Significant extensions and improvements to existing detection schemes are needed if they are to be used in multi-hop CR networks. Existing research results indicate that a detection framework based on statistical inference theory—specifically sequential analysis [18]—may be most appropriate to detect the types of attacks discussed in this paper.

VII. Conclusion

In this paper, we have investigated two types of MAC layer misbehaviors that pose a threat to multi-hop CR networks: MAC-layer DoS attacks and MAC-layer selfish misbehaviors. In a DoS attack, an adversarial node transmits spurious control frames to saturate the common control channel, thus crippling the dynamic channel assignment mechanism of a given network. Our simulation results have indicated that such an attack can severely degrade the end-to-end throughput of packet flows without requiring the attacker node to transmit a large volume of spurious control frames. In the second type of misbehavior that we have identified, a selfish node refuses to forward packets for other nodes by reporting false information about channel availability during the channel negotiation process.

We have also discussed potential countermeasures against such MAC-layer misbehaviors. A scheme for authenticating MAC control frames would resolve most of the security issues raised in this paper, but it would not be a practical solution since a key management infrastructure is required to support such a scheme. Establishing and maintaining a key management infrastructure in a multi-hop network is very difficult. Another approach for addressing the security concerns raised in this paper is to employ detection schemes capable of detecting MAC-layer misbehaviors and identifying attacker nodes. More research is needed, however, to make such schemes feasible for multi-hop CR networks.

References

[1] J. Mitola, "Cognitive radio: an integrated agent architecture for software defined radio," *PhD Dissertation*, Royal Institute of Technology (KTH), Stockholm, Sweden, June 2000.

[2] B. Wild, K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *Proc. DySPAN*, Nov. 2005, pp. 124–130.

[3] P. Pawelczak, "Protocol Requirements for Cognitive Radio Networks (Freeband/AAF/D4.11)" Enschede: Freeband, 2005. Available at: https://doc.freeband.nl/dscgi/ds.py/Get/File-60831.

[4] Liangping Ma, Xiaofeng Han, Chien-Chung Shen**, "**Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks," *Proc. DySPAN*, Nov. 2005, pp. 203- 213.

[5] P. Pawelczak, R.V. Prasad, Xia Liang, I.G.M.M. Niemegeers, "Cognitive radio emergency networks - requirements and design," *Proc. DySPAN*, Nov. 2005, pp. 601- 606.

[6] IEEE 802.22 Working Group on Wireless Regional Area Networks, "IEEE P802.22/D0.1 Draft Standard for Wireless Regional Area Networks Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands." IEEE doc: 22-06-0067-00-0000_P802-22_D0.1, May 15th, 2006.

[7] Jungmin So, and Nitin H. Vaidya. "Multi-channel mac for ad hoc networks: handling multi-channel hidden terminals using a single transceiver." *Proc. of MobiHoc*, May 2004

[8] IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specification, 802.11, 1999.

[9] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," *IEEE Transactions on Mobile Computing*, Vol. 4(5), Sept.-Oct. 2005, pp. 502–516.

[10] V. Gupta, S. Krishnamurthy and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *Proc. of MILCOM*, 2002, pp. 1118-1123.

[11] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proc. of USENIX Security Symposium*, San Antonio, TX, June 2003.

[12] M. Raya, J.P. Hubaux and I. Aad, "DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots," *Proc. of MobiSys*, June 2004.

[13] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. of IEEE INFOCOM* , March 2005, Vol. 4, 13-17, pp. 2513 – 2524.

[14] Shih-Lin Wu, Chih-Yu Lin, Yu-Chee Tseng and Jang-Laing Sheu, "A new multi-channel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks," in *Proc. of International Symposium on Parallel Architectures, Algorithms and Networks*, *I-SPAN*, 2000.

[15] Carlos Cordeiro, Kiran Challapali, Dagnachew Birru and Sai Shankar N. "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," in *JOURNAL OF COMMUNICATIONS (JCM).* Vol. 1(1), April 2006, pp. 38-47

[16] R. Jain. *The Art of Computer System Performance Analysis*.John Wiley and Sons, Inc., 1991.
[17] S. Radosavac, J. S. Baras, and I. Koutsopoulos, "A framework for MAC protocol misbehavior detection in wireless networks," in *Proc. of the 4th ACM Workshop on Wireless Security (WiSE '05*), Sep. 2005, pp. 33–42.
[18] A. Wald. *Sequential Analysis*. John Wiley and Sons, New York, 1947.