Covert Spectrum Handoff: An Attack in Spectrum Handoff Processes in Cognitive Radio Networks

Moinul Hossain and Jiang Xie
Department of Electrical and Computer Engineering
The University of North Carolina at Charlotte
Email: {mhossai4, Linda.Xie}@uncc.edu

***Abstract*—Spectrum handoff is an integral part of a cognitive radio-based network (CRN). It ensures the operational integrity of opportunistic spectrum access, the avoidance of harmful interference with licensed or primary users (PUs), and the delay requirement during a handoff. However, due to the random nature of PU activity, interference between primary and secondary users (SUs) are difficult to prevent. Proactive spectrum handoff aims to control this harmful interference between PUs and SUs by predicting the future activity of PUs and initiating spectrum handoff before a PU reappears. Though a few security aspects of CRNs attracted attention of researchers, vulnerabilities in the distributed proactive spectrum handoff process remain unstudied. In this paper, we introduce a vulnerability in the proactive spectrum handoff process and demonstrate how a selfish attacker can exploit this vulnerability to achieve personal gain. We name this *covert spectrum handoff*. To the best of our knowledge, this is the first work to consider security aspects of spectrum handoffs and to introduce an attack in the proactive spectrum handoff process.**

I. Introduction

The constrained amount of radio resource has made it a challenge to meet the ever-increasing demand for wireless services. However, there exist spectral inefficiencies in terms of the allocated bandwidth and traffic volume. Cognitive radio (CR) offers a solution to this challenge by enabling opportunistic access to underutilized radio resources. One of the most fundamental functionalities of CR-based networks (CRNs) that resolves this challenge is *spectrum mobility* [1], which enables secondary users (SUs) to change their operating channel based on the spectrum availability around them. In addition, it introduces a new type of handoff called *spectrum handoff*, which refers to the process that, when the current transmitting channel of a SU is no longer available, the SU needs to suspend its on-going transmission, to vacate the channel, and to determine a target channel to resume its transmission. However, due to the randomness in primary user (PU) activities, it is difficult to achieve fast and smooth spectrum transition, which can ensure limited interference to PUs and manageable performance degradation of SUs.

Currently, research on spectrum handoffs in CRNs falls into two approaches based on the moment when SUs initiate handoffs. In the *reactive* approach, SUs perform spectrum switching and Radio Frequency (RF) front end reconfiguration after detecting a PU reappearance. In the *proactive* approach, SUs predict the future channel activity and initiate spectrum switching and RF reconfiguration before a PU reappears in the current channel (based on observed channel usage statistics). Though both approaches have different strengths, when ensuring permissible interference to PUs, the proactive approach works better than the reactive approach [2].

Motivations: In prior research, most works either considered the availability of a dedicated common control channel (CCC) to exchange control information [3]–[6] or considered spectrum handoff without one [7]–[9]. In reality, due to the difference in spectrum usage by PUs (in both space and time), spectrum availability may differ depending on SU locations and a single common channel may not be available. Hence, two SUs must find a common available channel between them to establish a connection. The state-of-the-art work usually proposes that two SUs hop onto different channels from one time slot to another (i.e., channel hopping process) until they rendezvous on a common available channel [10], and they can exchange control information afterwards.

Moreover, most related works on spectrum handoffs and rendezvous processes had assumed identical channels in terms of service rate [2], [7], [11]–[16] (i.e., all channels have equal bandwidth). In reality, the available channels are not always going to be identical, and we must consider the diversity in service rate to manage handoff more efficiently (e.g., a faster target channel could compensate the handoff delay). Furthermore, in existing proactive handoff approaches, a handoff is triggered only when an SU finds the current channel unavailable for the next frame. Otherwise, it keeps transmitting on the current channel until all frames end.

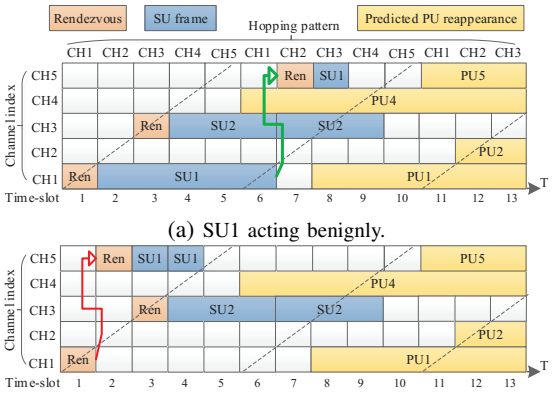
The concepts of channel hopping, rendezvous, spectrum handoff, non-identical channels, and handoff trigger time have mostly been studied in isolation. In reality, we must consider these functionalities together in a CRN and identify vulnerabilities before designing corresponding network protocols.

Challenges: Prior research considered the security aspect of spectrum sensing only, such as the primary user emulation attack [17], the sensing data falsification attack [18], and the off-sensing attack [19], [20]; however, vulnerability in spectrum handoff processes remain unstudied. In addition, though a few papers have considered some of the mentioned functionalities together, no work has addressed all of these. Hence, unavailability of relevant research work poses a significant challenge to address security vulnerabilities under realistic scenarios.

Contributions: When we consider all these functionalities together, it engenders a novel vulnerability in the proactive spectrum handoff process where an *attacker* (or a selfish SU)

This work was supported in part by the US National Science Foundation (NSF) under Grant No. 1343355, 1718666, 1731675.

978-1-5386-4727-1/18/$31.00 ©2018 IEEE



(a) SU1 acting benignly.

(b) SU1 acting selfishly.

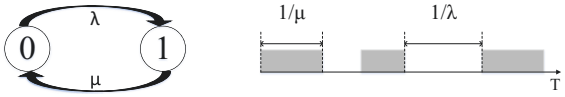
Fig. 1: The covert spectrum handoff in the proactive handoff process.

can trigger an early handoff to reserve the best available channel sooner than benign SUs. We provide an illustration of the vulnerability in Fig. 1. Here, we assume a common-hopping sequence-based rendezvous method and show activity in five channels with non-identical service rates. We consider that each SU packet consists of two frames, that a transmission attempt must be preceded by a rendezvous, and that SUs must follow the hopping pattern to initiate a new packet transmission. The SU frame length in CH1, CH2, CH3, CH4, and CH5 is 5, 4, 3, 2, and 1 time-slots long, respectively. Here, dotted lines represent the hopping pattern. In Fig. 1(a), we can see SU1 switching from CH1 to CH5 (in slot-7) as it predicts an imminent reappearance of PU1 after transmitting the first frame. To select the target channel, SU1 finds the channel that is not occupied by any SU (e.g., CH3 occupied by SU2), is least likely to affect by returning PUs, and has a faster service rate. Hence, SU1 selects CH5 as the target channel.

In contrast, a selfish SU can initiate a handoff promptly after the first rendezvous (Fig. 1(b)) and reserve CH5 sooner (in slot-2). In doing this, the selfish SU is motivated to finish its transmission faster (4 time-slots faster in the example) rather than acting benignly. We name this selfish attack *covert spectrum handoff*, which represents performing spectrum handoff secretly to gain access to the best available channel sooner, and we call this scenario *prompt proactive spectrum handoff*. The novel contributions of this paper are:

1. We introduce a new attack in the proactive spectrum handoff process, which exploits vulnerabilities in proactive spectrum handoff approaches.
2. We consider rendezvous, channel sensing, network coordination, and spectrum handoff together from a security perspective.
3. We show the severe impact of our proposed attack in cognitive radio ad-hoc networks (CRAHNs) through extensive simulation and analysis.

Related Work: In [2], a distributed proactive spectrum handoff process and a channel selection scheme are proposed. It considers most functionalities that we mentioned earlier in this section. In [3], a Hidden Markov model-based prediction is used to provide a smart spectrum mobility scheme. It considers the idle duration of the channel and the reappearance probability of PUs in the channel to perform proactive handoffs. In [4], a voluntary spectrum handoff is proposed where SUs perform handoff voluntarily to reduce the handoff and channel selection delay based on probabilistic methods. In [7], a preemptive resume priority-based M/G/1 queuing model is proposed to minimize the total service time of SUs. Nonetheless, the queuing model is not distributed and considers a central authority to maintain the queue. Moreover, the model does not consider a CCC and network coordination in the design. In [12], a distributed proactive spectrum handoff and channel selection method is proposed. It incorporates the channel rendezvous and the network coordination issue together in the spectrum handoff process. However, it does not consider collisions between SUs in multi-handoff scenarios.



(a) Transition rate. (b) PU activity in the time line.

Fig. 2: PU activity model.

Though all mentioned works contribute to the spectrum access in CRAHNs, no work has considered non-identical channels and the effect of non-identical channels in spectrum handoff decisions. In addition, security concerns of the proactive spectrum handoff process are overlooked.

II. System Model

A. PU and SU Model

We consider that all PUs are under the sensing range of SUs and that PUs do not interfere with each other's transmission. Here, M channels (i.e., M PUs) have different service rates, and a PU randomly selects a channel to access. N SUs can opportunistically access these M channels. An SU can access a channel when it senses no PU is using it. In addition, an SU can detect a collision with a PU only after the SU finishes the frame transmission (e.g., if an ACK is not received). After detecting a collision, the SU stops transmitting on the current channel and initiates a spectrum handoff. Each SU is equipped with one radio for spectrum sensing and one radio for control information exchange and data transmission. The sensing radio has two key functions: 1) observe the channel usage characteristics and store the channel statistics to predict future channel activity and 2) confirm that the newly selected channel is idle for the transmission of SU.

Each PU alternates between the ON and OFF state according to a continuous-time Markov process. In Fig. 2, let λ and μ denote the transition rate from the OFF to ON state and from the ON to OFF state, respectively. Thereby, the mean sojourn time in the ON and OFF states is $1/\mu$ and $1/\lambda$, respectively, and both follow the exponential distribution.

B. Network Coordination Scheme

Rendezvous is a prerequisite in establishing a connection between two SUs in the absence of a dedicated CCC. A successful rendezvous happens when both transmitting and receiving SUs are on the same channel and have completed a successful handshake between them, e.g., a Request-to-Send/Clear-to-Send (RTS/CTS) exchange.

We consider the common channel-hopping as the network coordination scheme [12], which means that the hopping

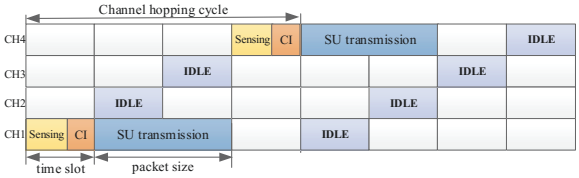
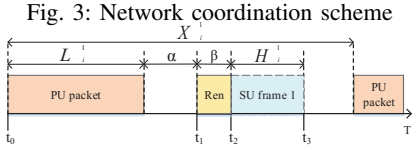
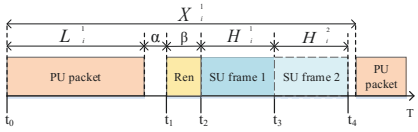


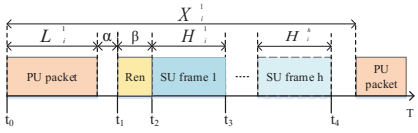
Fig. 3: Network coordination scheme



(a) SU sending the 1st frame.



(b) SU sending the 2nd frame.



(c) SU sending the hth frame.

Fig. 4: PU and SU Activity on channel i

pattern is the same for all SUs. Fig. 3 illustrates the operation of the common frequency-hopping network coordination. We consider a time-slotted system. Each time-slot consists of a sensing interval (sensing) and a contention interval (CI) with the transmission of an RTS/CTS pair. When there is no packet in the buffer of an SU, it keeps hopping through the channels from one time-slot to another, based on the predetermined common channel-hopping pattern. Then, we adopt the MAC model from [13] for network coordination. Whenever an SU has a packet to send, it first senses the channel. If the channel is idle, the SU chooses a random number (in terms of mini-slots) as its backoff time to avoid contention.

C. Proactive Spectrum Handoff Model

Proactive spectrum handoff helps to decrease the unwanted interference between PUs and SUs. In this section, we briefly discuss the proactive model we use in our simulations.

We consider that each SU calculates the likelihood of PU reappearance after performing a successful rendezvous. Using the sensed channel statistics, an SU can predict the channel availability before the transmission of the current frame ends. Based on the prediction, an SU decides whether to transmit on the current channel, switch to another channel, or pause the on-going transmission and remain on the current channel. We set a threshold (τ) for PU reappearance, above which an SU will not initiate the transmission. Fig. 4 shows the PU and SU traffic activity on channel i, where X_i^k represents the inter-arrival time of the k^{th} PU packet on channel i. L_i^k and H_i^k denote the length of the k^{th} PU and k^{th} SU packet on channel i, respectively. Here, t_0 represents the last sensed arrival of a PU packet and $N_i(t)$ denotes the status of PU reappearance within time t. $N_i(t)$ is a binary random variable with values 0 and 1, representing no PU reappearance and PU reappearance, respectively. As shown in Fig. 4(a), the probability that channel i will be idle till the first frame ends (t_3) is given by,

$$Pr(N_i(t_3) = 0) = Pr(X_i^1 > L_i^1 + \alpha + \beta + H_i^1). \quad (1)$$

where β and α represent the time to successfully perform a rendezvous (i.e., 1 time slot), and the time between when the PU packet finishes the transmission and the rendezvous starts, respectively. In Fig. 4(b), the probability that channel i will be idle till the second frame ends (t_4) is given by,

$$Pr(N_i(t_4) = 0) = Pr(X_i^1 > L_i^1 + \alpha + \beta + H_i^1 + H_i^2). \quad (2)$$

Therefore, the probability that an SU successfully transmits a packet on channel i, consisting of h frames, (Fig. 4c) is,

$$Pr(N_i(t_4) = 0) = Pr(X_i^1 > L_i^1 + \alpha + \beta + \sum_{l=1}^{h} H_i^l). \quad (3)$$

Hence, based on the above predictions, the probability that an SU will handoff to a new channel is,

$$Pr(N_i(t) = 1) = 1 - Pr(N_i(t) = 0) > \tau. \quad (4)$$

Here, we consider the same threshold to make the decision on whether to switch from the current channel and to select a target channel. Every transmission on a new channel must be preceded by a sensing and contention attempt (i.e., rendezvous). In addition, the highest priority to access channels is given to handoff SUs to maintain low handoff delays.

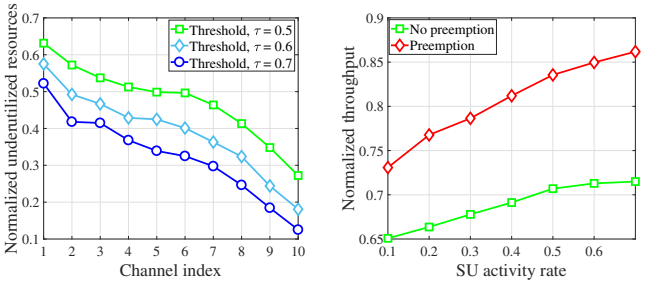
III. Covert Spectrum Handoff

Although the distributed nature of proactive spectrum handoff processes provide such protocols with significant performance gain in terms of avoiding collisions with PUs, it also exposes such approaches to new security vulnerabilities (e.g., covert spectrum handoff). In this section, we first identify the motivating reasons to exploit this vulnerability and then discuss the strategy of an attacker. We consider that a selfish SU is compromised, is authorized to use the secondary network, and has similar hardware configurations as benign SUs. To exploit this vulnerability, both transmitter and receiver SU must act selfishly. Throughout this paper, we will use the term *attacker* and *selfish SU* interchangeably.

A. Vulnerability Analysis

Here, we shed light on the reasons behind this vulnerability and how a selfish SU can remain undetected in current proactive approaches.

Underutilized Radio Resources: Previous works on rendezvous ([13], [14], [21]) focus only on achieving guaranteed and fast rendezvous. However, the radio resource utilization is not considered as a performance metric. SUs' waste radio resources in the rendezvous process until they successfully handshake with each other. Fig. 5(a) shows the amount of wasted radio resources in the common-hopping sequence-based rendezvous system in saturated SU traffic (i.e., SUs always have a packet to send). We consider non-identical service rates for each channel ranging from 1 to 10 Mbps for channel-1 to channel-10, respectively (i.e., channel-1 offers the lowest service rate and channel-10 offers the highest). Here, we show the normalized wasted radio resources of each channel and vary the value of threshold (τ) to observe the channel wastage trend. It clearly exhibits the ramifications of using the periodic hopping sequence approach, even with a higher threshold and saturated SU activity.



(a) Underutilized resources. (b) Conventional vs. Prompt.

Fig. 5: The motivating reasons behind the attack.

Less Prompt in Handoff Initiation: As we discussed in the introduction, most proactive handoff processes trigger handoff only when the next frame is likely to collide with a reappeared PU on the channel. As they consider identical channels and emphasize on reducing the delay constituting from handoff operations, prior handoff processes are inherently reluctant to handoffs. However, if we consider non-identical channels, it is likely to manage a trade-off between the delay constituting from switching to a faster channel and the service rate of that channel. In this process, an SU can initiate the handoff process instantly after the rendezvous (if a faster channel is available to off-set the handoff delay), and we call it preemptive proactive handoff process. In Fig. 5(b), we can observe a significant increase in the normalized throughput between the conventional and preemptive proactive handoff process. Here, the preemptive process considers non-identical channels, likelihood of PU reappearance, and channel bandwidth as handoff criteria. Therefore, this finding indicates that the preemptive trigger offers a sizable performance gain for an attacker if it exploits this vulnerability.

Absence of a Central Entity: The absence of a central entity in CRAHNs makes it difficult to detect an attacker with selfish intentions. Current research on the detection and defense of deviant behaviors in distributed networks are based on long-term monitoring of neighboring nodes and exchanging this monitored information with each other to make a consensus [22]–[24]. However, this is difficult to perform in a network without a dedicated CCC, especially when the attacker and defenders are not on the same channel. Here, the attacker avoids detection by covertly utilizing channels that are not currently used by any SUs.

These three aspects of distributed CRNs can motivate an SU to deviate from established protocol and to act selfishly.

B. Attacker Model

The attacker acts benignly during the hopping process to avoid suspicion. It starts to exploit the vulnerability only after performing a successful rendezvous (Fig. 1(b)). According to the common-hopping process, an SU pair stays on the rendezvous channel and initiates a transmission, and other SUs hop to the next channel in the sequence. Prior defense techniques against selfish SUs work only if they would stay on the same channel. Therefore, the integral part of remaining undetected is to handoff to a channel that is not used by any other SU (e.g., the subsequent channel in the hopping sequence).

However, after a successful rendezvous, the attacker pair tries to search for a better channel to switch. The strategy of the proposed attack model is given in Algorithm 1.

Algorithm 1 Attacker's Activity

Input: hopping sequence S, time t, PU reappearance threshold τ
Result: $decision$
$rendezvous\_status := unsuccessful$;
while $rendezvous\_status = unsuccessful$ **do**
  $i := (t-1)\%length(S)+1$; ▷ follow channel-hopping
  $currnet\_channel := S(i)$;
  if *current_channel=free & contention_status=win* **then**
    $rendezvous\_status := successful$;
    $r_{ch} := current\_channel$;
  else
    $t := t+1$; ▷ proceed to the next time-slot
  end
end
$C :=$ ComputeTargetChannel(S,t,r_{ch});
$decision :=$ HandoffPreemption (C,r_{ch},τ);

Preceded by a successful rendezvous, the attacker pair tries to find a suitable target channel. Algorithm 2 shows the pseudocode of the channel selection process. It first sorts all the channels according to the prediction of PU reappearance and service rate in each channel, then starts checking them one by one to select the most suitable target channel.

Algorithm 2 Computing the Target Channel for Selfish SU

Input: hopping sequence S, time t, rendezvous channel r_{ch}
Result: target channel C
function COMPUTETARGETCHANNEL(S,t,r_{ch})
$CH := sort\ channels\ according\ to\ the\ likelihood\ of\ PU\ reappearance\ and\ service\ rate$;
$j := 1$;
while $CH(j) = busy \| CH(j) = next\ channel\ in\ sequence$ **do**
  $j := j+1$;
end
return $C := CH(j)$;

The criteria for selecting the most suitable channel is described in the steps below.

Less Likely to Be Affected by Reappeared PUs: By utilizing the in-hand resources of proactive handoff, the attacker pair can calculate the probability of PU reappearance in each channel. Then, they will try to reserve the channel that offers the least likelihood to be affected by a returning PU.

Faster Service Rate: An attacker's motive is to finish packet transmission sooner and to maximize its own channel utilization. After performing a successful rendezvous on channel i, the target channel j needs to maintain the inequality condition,

$$\epsilon_{ij} + L_j < L_i, \tag{5}$$

where L_i and L_j represent the packet length of the attacker in channel i and j, respectively, and ϵ_{ij} represents the delay of performing a handoff from channel i to channel j.

Not Being Used by Other SUs: The attacker pair will avoid channels that are already being used by other SUs. However, such avoidance can ensure the availability of a corresponding channel only in the current time-slot and there is a probability that another SU might handoff to the same channel in the next time-slot; hence, they need to contend to reserve the channel. Moreover, the attacker will not handoff to the channel that comes next in the hopping sequence. In Fig. 1(b), the selfish SU would not handoff to CH2 from CH1 to avoid suspicion.

Finally, the handover decision of the attacker pair depends on the target channel. If they are currently operating on the best available channel, then they do not perform a handoff. Algorithm 3 shows the pseudocode of the handoff preemption decision process. The attacker pair will handoff to a channel only if the channel satisfies the earlier mentioned criteria. Otherwise, the attacker pair will stay on the current channel.

Algorithm 3 Handoff Preemption Decision

Input: target channel C, rendezvous channel r_{ch}, threshold τ
Result: *decision*
function HANDOFFPREEMPTION(C,r_{ch},τ)
if C=r_{ch} **then**
  $handoff\ preemption := 0$; ▷ no preemption
else
  $handoff\ preemption := 1$; ▷ activate preemption
end
if *handoff preemption=0* **then**
  if *prediction*(r_{ch}) $\leq \tau$ **then**
    $decision := begin\,transmission$;
  else
    $decision := stay\,idle\,and\,wait\,for\,a\,better\,channel$;
  end
else
  if *prediction*(C) $\leq \tau$ **then**
    $decision := handoff\,to\,C$;
  else
    $decision := stay\,idle\,and\,wait\,for\,a\,better\,channel$;
  end
end
return *decision*

In our model, we consider that the attacker pair initiates a preemptive handoff only after rendezvous, and they refrain from searching for better channels for each successive frames. Otherwise, attackers are likely to lose their opportunity to transmit, to become trapped in a loop of handoffs, and to increase handoff delay significantly.

IV. Performance Analysis

In this section, we evaluate the impact of the proposed covert spectrum handoff by conducting extensive simulations. The parameters used to obtain the simulation results are listed in Table I. The arrival of PU and SU packets follow the Poisson process, and the length of PU and SU packets are exponentially distributed and fixed, respectively. As the attacker pair initiates its malicious act only after the rendezvous and does not continue it for each subsequent transmitting frame, we consider a packet as 1 frame length long to analyze the performance. In the simulation, we consider one pair of attacker if not stated otherwise.

TABLE I: Simulation Parameters

Simulation area	500x500
Simulation time	50 sec
The number of PUs	10
The number of SUs	50
Number of channels	10
Channel data rate	1-10 Mbps
The size of (RTS+CTS)	160 + 112 bits (802.11b/g)
PU ON time	0.5 (uniform for all PUs)
SU traffic rate	0.1-0.7 (uniform for all SUs)
Length of a time slot	1.5ms
Frame length	1-10 time slot long

Increased Average Throughput: One important metric to evaluate the performance of this attack is throughput. In Section III, we discussed the difference in throughput between the conventional and the preemptive handoff initiation. However, earlier we considered that all SUs follow the preemptive handoff initiation process. In this section, we consider that only the attacker pair follows the preemptive handoff initiation process, and benign SUs follow the conventional process.

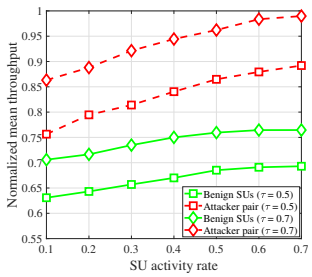
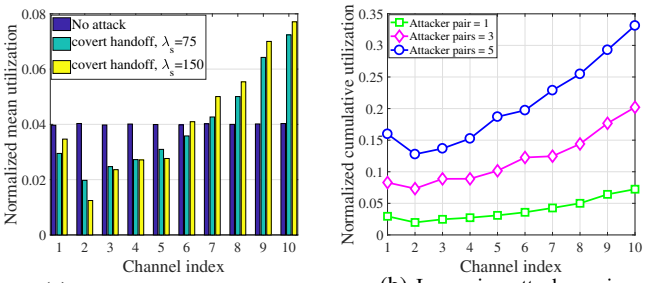


Fig. 6: Normalized average throughput of benign SUs vs. the attacker pair.



(a) With vs. without attack. (b) Increasing attacker pair.

Fig. 7: Normalized average channel utilization of benign SUs and attackers.

Fig. 6 illustrates a throughput gain ($19 - 30\%$) by the attacker pair compared to benign SUs. As the attacker pair preempts handoff process and reserves a channel with faster service rate earlier, it experiences significantly higher throughput. Moreover, benign SUs experience less room to utilize faster channels as the attacker pair utilizes faster channels more often. Therefore, we can observe an increase in attackers performance from Fig. 5(b) to Fig. 6.

Higher Channel Utilization of Faster Channels: As discussed, the attacker pair always tries to reserve the best available channel by initiating the handoff process earlier (i.e., preemption). In Fig. 7(a), we can observe the channel utilization by the the attacker pair in no-attack and attack scenarios. In the benign scenario, they use all the channels uniformly, and this uniformity represents the fairness in the system. However, after they become selfish (i.e., preemption in handoff), the utilization of faster channels by the attacker pair increases. In addition, we observe an increase in the utilization, as we increase the traffic rate of selfish SUs.

In Fig. 7(b), the impact of increasing the number of attackers on the channel utilization is shown. As the number of attackers increases, they occupy the faster channels more, and it increases the cumulative channel utilization of attackers. If we consider 5 pairs of attackers among 50 SUs, then it shows the utilization of channel-10, approximately 33% (i.e., 20% nodes are utilizing 33% radio resource).

Higher Collision Avoidance: In the process of increasing the throughput, the attackers are inherently avoiding collisions with reappeared PUs. As the covert spectrum handoff (or

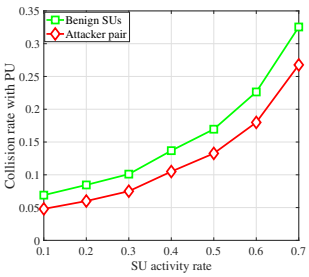
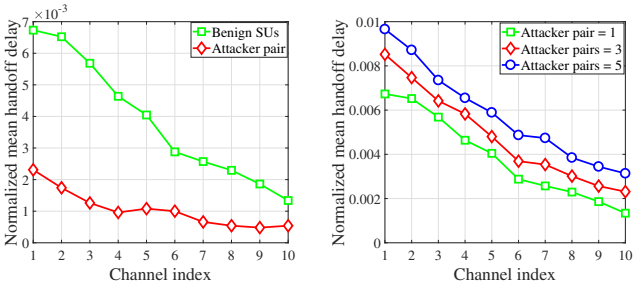


Fig. 8: Normalized average collision rate of benign SUs vs. attackers.



(a) Benign SUs vs. selfish SUs. (b) Delay of benign SUs.

Fig. 9: Normalized average handoff delay of benign SUs and selfish SUs.

preemptive handoff) happens only to a faster channel that offers less probability of PU reappearance, attackers increase their throughput and ensure less collisions from PUs. In Fig. 8, the collision rate with PUs are shown and we can observe a reduction in the collision rate between PUs and SUs.

Handoff Delay: We observe a reduction in the average handoff delay of the attacker pair compared to benign SUs. Though it might seem that attackers perform more handoffs, their propensity toward faster channels with lower PU reappearance probability ensures that they experience fewer handoffs later in the transmission time. In Fig. 9(a), the normalized average delay of the benign and selfish SUs are demonstrated. Here, channel index represents the channels that handoff initiated from, not the target channel. Therefore, it indicates that more handoff takes place in slower channels, which is expected.

Moreover, in Fig. 9(b), as the number of attackers increases, they occupy faster channels more. Therefore, benign SUs are deprived from utilizing faster channels, and sometimes they are forced to stop transmissions due to the unavailability of a channel. Moreover, as handoff SUs are given higher priority to access a channel, benign SUs lose contention to attackers; hence, benign SUs waste more time in the handoff process to transmit each packet.

V. Conclusion

In this paper, we introduced a novel attack, which exploits a vulnerability in existing spectrum handoff processes. Here, attackers maximize their personal gain by preempting the channel switching process. As they strategically avoid channels where benign SUs are trying to rendezvous and transmit, attackers remain undetected. We made an strategy to exploit this vulnerability and analyzed the impact of this attack through simulations. While we discussed the impacts, we also identified the reasons behind this vulnerability. This is the first work to introduce a vulnerability in the spectrum handoff process in CRNs.

References

[1] I. F. Akyildiz *et al.*, "A survey on spectrum management in cognitive radio networks," *IEEE Communications magazine*, vol. 46, no. 4, 2008.

[2] Y. Song and J. Xie, "ProSpect: A proactive spectrum handoff framework for cognitive radio ad hoc networks without common control channel," *IEEE Transactions on Mobile Computing*, vol. 11, no. 7, pp. 1127–1139, 2012.

[3] I. A. Akbar and W. H. Tranter, "Dynamic spectrum allocation in cognitive radio using hidden markov models: Poisson distributed case," in *Proc. IEEE SoutheastCon*, 2007, pp. 196–201.

[4] S.-U. Yoon and E. Ekici, "Voluntary spectrum handoff: a novel approach to spectrum management in CRNs," in *Proc. IEEE ICC*, 2010, pp. 1–5.

[5] Y. Zhang, "Spectrum handoff in cognitive radio networks: Opportunistic and negotiated situations," in *Proc. IEEE ICC*, 2009, pp. 1–6.

[6] S. Geirhofer, J. Z. Sun, L. Tong, and B. M. Sadler, "Cognitive frequency hopping based on interference prediction: Theory and experimental results," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 49–61, 2009.

[7] C.-W. Wang and L.-C. Wang, "Modeling and analysis for proactive-decision spectrum handoff in cognitive radio networks," in *Proc. IEEE ICC*, 2009, pp. 1–6.

[8] L. Yang, L. Cao, and H. Zheng, "Proactive channel access in dynamic spectrum networks," *Physical Communication*, vol. 1, no. 2, pp. 103–111, 2008.

[9] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE ICC*, vol. 4, 2006, pp. 1658–1663.

[10] X. Liu and J. Xie, "A practical self-adaptive rendezvous protocol in cognitive radio ad hoc networks," in *Proc. IEEE INFOCOM*, 2014, pp. 2085–2093.

[11] Y. Song and J. Xie, "Performance analysis of spectrum handoff for cognitive radio ad hoc networks without common control channel under homogeneous primary traffic," in *Proc. IEEE INFOCOM*, 2011, pp. 3011–3019.

[12] ——, "Common hopping based proactive spectrum handoff in cognitive radio ad hoc networks," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

[13] X. Liu and J. Xie, "Contention window-based deadlock-free MAC for blind rendezvous in cognitive radio ad hoc networks," in *Proc. IEEE GLOBECOM*, 2015, pp. 1–6.

[14] ——, "A slot-asynchronous MAC protocol design for blind rendezvous in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2014, pp. 4641–4646.

[15] J. Xie, "User independent paging scheme for mobile IP," *Wireless Networks*, vol. 12, no. 2, pp. 145–158, 2006.

[16] J. McNair, T. Tugcu, W. Wang, and J. L. Xie, "A survey of cross-layer performance enhancements for mobile IP networks," *Computer Networks*, vol. 49, no. 2, pp. 119–146, 2005.

[17] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[18] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE GLOBECOM*, 2009, pp. 1–6.

[19] M. Hossain and J. Xie, "Impact of off-sensing attacks in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2017, pp. 1–6.

[20] ——, "Off-sensing and route manipulation attack: A cross-layer attack in cognitive radio based wireless mesh networks," in *Proc. IEEE INFOCOM*, 2018.

[21] X. Liu and J. Xie, "Subset: A joint design of channel selection and channel hopping for fast blind rendezvous in cognitive radio ad hoc networks," in *Proc. IEEE SECON*, 2015, pp. 426–434.

[22] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 8, no. 1, pp. 1–24, 2008.

[23] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *Proc. IEEE International Symposium on Integrated Network Management (IM)*, 2015, pp. 606–611.

[24] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.