ARTICLE IN PRESS

Computer Networks xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey Paper

A layered approach to cognitive radio network security: A survey

Deanna Hlavacek *, J. Morris Chang [1]

Department of Electrical and Computer Engineering, Iowa State University, United States

ARTICLE INFO

Article history:
Received 24 September 2013
Received in revised form 6 August 2014
Accepted 1 October 2014
Available online xxxx

Keywords:
Cognitive
Radio
Security
Spectrum
Wireless
Network

ABSTRACT

Cognitive radios have been identified as a solution to the crowded spectrum issue. With the realization of cognitive radio networks came the recognition that both new and old security threats are relevant. The cognitive radio network is still vulnerable to many of the denial of service, wormhole, routing, and jamming attacks that plague other wireless technologies. In addition, the cognitive radio network is vulnerable to new attacks based on cognitive radio innovations, such as spectrum sharing, spectrum sensing, cognitive capability, and radio reconfigurability. The scope of this survey is to present an overview of security threats and challenges to the cognitive radio network, especially focusing on new solutions from 2012 and the first half of 2013. Included are prior mitigation techniques that are adaptive to the new technology, as well as new mitigation techniques specifically targeted at new cognitive radio vulnerabilities. The threats provided are organized according to the protocol layer at which the attack is targeted.

1. Introduction

It has been estimated that the people of the United States are now outnumbered by their wireless devices. The proliferation of wireless devices such as laptops, notebooks, cellular phones, smart phones, and tablets has caused the frequency spectrum used for transfer of information to become crowded [70]. Also, the expected growth in media-rich consumer applications and wireless data transfer will continue to further crowd the network, making additional spectrum throughput a priority.

Currently in the United States spectrum is allotted to various services in three main categories: licensed, lightly licensed, and unlicensed [1]. Licensed spectrum refers to the portions of the spectrum reserved by each country's equivalent of the Federal Communications Commission (FCC) for specific uses, such as military, public safety, and commercial uses. Lightly licensed spectrum refers to the bands that are generally regulated for licensed users, with regional or other exceptions. In the unlicensed band there are predefined technical rules for the hardware and radio technology intended to mitigate interference between the bands. The spectrum is available for network setup by any person or entity, public or private, to include commercial high speed internet, provided that it does not infringe upon the band's rules [1].

In an effort to provide relief to the users of the overused spectrum, in 2010 the FCC allocated unused spectrum between television channels, or "white spaces" for unlicensed use. In addition, the FCC has proposed setting aside some low band spectrum, and possibly underutilized portions of the military, amateur radio, and paging frequencies, for unlicensed use as long as the primary user experiences no interference. Finally, in early 2013, the

* Corresponding author at: Iowa State University, Ames, IA 50014, United States.
E-mail addresses: deannah@iastate.edu (D. Hlavacek), morris@iastate.edu (J.M. Chang).
[1] Tel.: +1 515 294 1097.

http://dx.doi.org/10.1016/j.comnet.2014.10.001
1389-1286/

FCC opened a process to allocate more high frequency spectrum for unlicensed use.

In addition to spectrum overcrowding, one of the major challenges for the wireless medium is security. The WiFi brand was adopted in 1999 based on the 802.11 standard. It was immediately realized that using the electromagnetic wave as the propagation medium made physical security of the transmitted data an impossibility. A conversation made of electromagnetic signals can be intercepted, jammed, or injected with extraneous bits. These actions can cause the release of private information, the inability to send and receive information, or the receipt of false or unreadable data.

As with other wireless communications, the cognitive radio technology based on the 802.22 standard must enforce the security triad of confidentiality, integrity, and availability (CIA). The cognitive radio is subject to many of the same types of attacks that plague other cellular and wireless communication systems. In addition, due to the cognitive radio's ability to self-organize a network and establish routing similar to wireless sensor networks (WSNs), the cognitive radio network (CRN) is also vulnerable to attacks originally designed for WSNs. Finally, the abilities of the CRN to sense the environment, adjust spectrum usage parameters, collaborate with neighbors, and learn provide new avenues for attack.

Because cognitive radio is in its infancy, there are many opportunities for research into the security issues to which the new technology is vulnerable. Such research can drive the creation of a more secure product. The papers [9,55,69] provide a general overview of the cognitive radio network model with a broad description of secure model considerations. The authors of [54] provide a very extensive overview of all cognitive radio network issues, with an in depth look at the security issues specific to the new CRN vulnerabilities.

The papers [41,91] each provide a high level view of the legacy and newer threats that can be applied to the cognitive network. The authors of [6,92] both take a broad stroke at listing and describing threats specific to the cognitive radio. In addition, the paper [6] adds a focus on the threats specific to the policy controlled cognitive radio. An in-depth look at the primary user emulation attack and mitigation is presented by the authors of [84,92]. The paper [74] analyzes vulnerabilities of existing spectrum sensing and access protocols under stochastic channels in the presence of jamming attacks. The authors of [78] concentrate on the vulnerabilities of the physical layer.

Comprehensive, security focused studies for the cognitive radio network were presented by [7,27,63,76]. The paper [76] takes the traditional approach of describing the possible attacks on a CRN. The authors of [7] categorize and analyze the threat vectors (as compared to attacks) and provides design considerations to alleviate the threats. A discussion on security evaluation and certification is included. Rather than analyzing the threats or attacks to the cognitive radio, the paper [27] analyzes the 2010 and earlier solutions presented to mitigate CRN security issues.

The paper [63] takes a layered approach in its study of cognitive radio network security. Four layers are presented: security applications, security strategies, security infrastructure, and security primitives. Threats are also presented in categories: learning, hidden node, policy, parameter, and sensing.

The security professional must be properly prepared for the battle that will ensue as the cognitive radio network comes into use. To that end, the purpose of this paper is to provide a survey of security issues related to the cognitive radio network. Potential attacks will be described, and proposed mitigation techniques will be explored. The attacks in the survey are presented according to the targeted protocol layer. Emphasis has been placed on presenting solutions proposed in 2012 and early 2013, when available. The remainder of the paper is organized as follows: Section 2 describes the general concepts and security considerations of the cognitive radio. Starting at Section 3 the paper presents attacks and mitigation techniques based on communication layer protocols. Sections 3–7 present the Physical layer, Data link layer, Network layer, Transport layer, and Application layer, respectively. Section 8 presents the Cross-layer attacks. Section 9 provides a conclusion. Table 1 will provide snapshots of the attacks presented by layer.

2. Cognitive radio

The cognitive radio is based on a software defined radio with adjustable operational parameters [2]. The software allows the radio to tune to different frequencies, power levels, and modulation schemes to establish or maintain a communication link. The hardware consists of an antenna, a radio frequency conversion module, a modem, and other modules [57]. The best configuration for the radio is determined by optimizing an objective function that considers such factors as interference and noise, traffic demand, mobility levels, and location.

In addition to the variable parameters mentioned above, the cognitive radio network is further adaptable to changing situations with its ability to operate successfully in collaborative (cooperative) or uncooperative networks. Generally, the throughput of the collaborative network will be higher than that of the uncooperative network due to the ability of the cooperating radios to share the frequency to which they will hop. However, when the network is under certain types of attacks, or in certain environmental situations, the uncooperative network configuration may be optimal. We must therefore analyze attacks and mitigation techniques for both scenarios.

It is generally agreed that the cognitive radio must provide the following functions: spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility. Spectrum sensing is required for the cognitive radio to sense the spectrum for the presence of the primary user or other traffic. Through spectrum management the radio is able to utilize the available spectrum efficiently without interfering with the primary user. The protocols established in the IEEE 802.22 standard govern the ability of the radio to share the spectrum with the primary user and other secondary users. The radio is able to vacate a spectrum when the primary user is indicated as present while continuing communication with the network due

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

Table 1
Attacks by layer.

Attacks by layer	Network member?	CIA	Description	Citation
PHY layer				
Jamming	External	A	Jammer maliciously sends packets to hinder legitimate spectrum usage	[10,11,26,47,50,61,71,79,80,82,83,93,96,101,111]
Objective function	Internal	A	Attacker manipulates transmission rate parameters so calculated results of the function are biased towards the attacker's interests	[5,13,18,44,81,103,106]
Overlapping secondary user	Both	A	A geographical region may contain overlapping secondary networks with a malicious user in one network transmitting signals that cause harm to the primary and secondary users of both networks	[97,109]
Primary user emulation	External	A	An external attacker emulates the signal of the primary user	[15,17,23,28–30,37,45,51,102,108,110,114]
Data link layer				
Byzantine	Internal	A	Attacker sends false local spectrum sensing results to neighbors/fusion center causing the receiver to make wrong spectrum sensing decisions	[3,21–23,25,31,35,39,46,56,60,62,65–67,73,105]
Control channel jamming	Both	A	Jamming of the control channel causes network confusion by interrupting the radio cooperation	[12,42,48–50,52,86,87,112]
Control channel saturation	Internal	A	Based on the fact that if a cognitive radio is unable to complete negotiations during the limited time of the control phase, the radio defers from transmission during the next data phase	[52,59]
Network layer				
HELLO flood	Internal	A	Node broadcasts HELLO loud enough so all nodes think it is a neighbor. Packets are lost since the node is far away	[24,40]
Ripple	External	A	The wrong channel information is provided so that the other nodes in the area change their channel. The attacker's intent is to cause the false information to be passed hop by hop and cause the network to enter a confused state	[115]
Sinkhole	Internal	C, I, A	Attacker advertises itself as the best route and does selective forwarding in which packets are modified or discarded	[40,100,107]
Sybil	Internal	A	Attacker sends packets as different identities subverting the trust system	[20,40,58,90,104]
Wormhole	Internal	C, I, A	Attacker tunnels messages or pieces of messages to different parts of network to replay them	[34,40]
Transport layer				
Key depletion	Internal	C, I	With the great number of session keys created in a cognitive radio network, it is very likely a key will be repeated. Repetitions provide an avenue to break the underlying cipher system	[53,72]
Application layer				
Cognitive radio virus	Both	A	The cognitive radio network is vulnerable to viruses that can effect radio function and learning	[18,32]
Policy attacks	External	A	Policy of the radio is changed or not allowed to be updated, providing the attacker unfair spectrum access	[6]
Cross-layer				
Jellyfish	Internal	A	Based on the dual role of the radio as router with forwarding behavior. The attack targets closed loop flows responsive to network conditions like delay and loss	[36,53,64,68,75]
Lion	External	A	Attack utilizes the PUE attack at physical layer to disrupt the TCP. TCP continues to create logical connections and send packets. The packets timeout, and TCP retransmits. Retransmit timer doubles with backoff resulting in delays and packet loss	[24,43]
Routing information jamming	Internal	A	A malicious node causes a targeted node to initiate spectrum handoff before the routing information is exchanged	[53,116]
Small backoff window	Internal	A	Node decreases its own backoff window size so it has a better chance of getting the channel	[98,113]

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

to the function of spectrum mobility. The spectrum functions required by the cognitive network radio add avenues of attack on the radio, network, and primary users in the area. These attacks may target (i) the spectrum sensing function by changing the spectrum environment, (ii) the decision making function by manipulation of parameters of the objective function, or (iii) the learning engine by providing false data about the environment that the learning radio will use in the future to make incorrect or inefficient decisions.

By classifying threats we can better determine threat severity, precautionary methods, and recovery strategies. Additionally, understanding the similarities between the threats can help us apply knowledge about previous attacks on other technologies to attacks on cognitive radio networks. The following framework provides a classification system for all cognitive radio network threats. The threats are classified according to the protocol layer upon which the attack is performed: physical layer (PHY), data link (or MAC) layer, network layer, application layer, and cross-layer. Cross-layer attacks are those in which the attack is launched utilizing one layer while the attack targets another layer. Basing the classifications upon protocol layers utilizes terminology already used in wireless communication security while simultaneously describing for the reader the attack vector. We start our discussion at the bottom of the layer stack and move upwards.

Table 1 lists each attack explored with the leg(s) of the CIA security triad affected by the attack. A majority of the attacks affect the availability of the cognitive radio services. Protecting the system availability basically includes protecting the common control channel from saturation, and ensuring the spectrum is sensed accurately and the members of the network are properly identified and provide accurate information. Ensuring confidentiality and integrity of the data transmitted is accomplished by encryption with a proper key distribution system, and proper identification and vetting of the network members. Mitigation of the attacks listed will help ensure secure communications.

3. Physical layer

The physical layer is the lowest layer of the protocol stack, providing an interface to the transmission medium. The physical layer consists of anything that is used to make two network devices communicate, such as the network cards, fiber, or, as in the cognitive radio network framework, the atmosphere. The operation of the cognitive radio network is more complicated than other wireless communication networks because the cognitive radio uses the frequency spectrum dynamically. Following are network attacks aimed at disrupting communication by targeting the physical layer of the cognitive radio network.

3.1. Primary user emulator attack

Testing results show that the number of dropped calls can be increased by up to two orders of magnitude due to primary user attacks [37]. Proper function of the spectrum sharing feature of the cognitive radio network requires the radio's ability to distinguish between the primary and secondary user signals. Techniques such as filter detection, energy detection, and cyclostationary-feature detection need to be leveraged to provide this distinction. In a hostile environment, discerning the primary user from others can become extremely difficult. In the primary emulation attack, an attacker may modify their air interface such that it emulates the primary user's signal characteristics causing other secondary users to falsely determine that the frequency is in use by the primary user, and so vacate the frequency. The imposter may perpetrate the attack selfishly, so he can use the spectrum, or maliciously, so the other legitimate users will have their communication disrupted, resulting in a denial of service attack. In addition, the attacker can poison the data collected about the spectrum usage that is used by the learning cognitive radio to determine which frequencies to try to access in the future. Therefore, the primary user attack (PUE) can lead to an objective function attack (Section 3.2) [102].

Determination that there is an imposter present in the network is the first step in mitigating the PUE attack. This subject falls into the area of robust distributed cooperative sensing and the detection of anomalies. Most anomaly detection is based upon statistical analysis of the sensed data. Localization of the malicious user can assist in the mitigation of the attack. The paper [51] provides a received signal strength indicator (RSSI) based transmitter localization technique that can be used when three or more trusted nodes are present. Triangulation with a correction technique considering multipath signals and refraction provides an improved localization method.

In a cooperative cognitive radio network each secondary user senses the spectrum periodically and reports the measurement results to the fusion center. The fusion center combines the data and makes a determination as to whether the primary user is present or not. If an attacker injects false positive offset data, the fusion center may determine the primary user is transmitting, when actually it is not. Conversely, if the attacker injects negative data, the fusion center may falsely determine the primary user is not present.

In [29] a differential game is proposed as an avenue for primary user emulation mitigation. Based on the differential attack game model the Nash equilibrium is derived, and the optimal attack/defense strategy is devised. Experimental results indicate that by using this strategy the secondary user can maximize the usability of the cognitive channels and minimize the disruption to the network caused by primary user emulation attacks.

In the paper [45] the authors introduce the robust principal component analysis (PCA) technique for spectrum sensing. The authors consider a cooperative cognitive radio network with one primary user, several nodes, and one fusion center. In the worst case PUE attack, the attacker would use tactics that include appearing intermittently and randomly to try to prevent discovery. This activity can be represented by a sparse matrix. Robust PCA is based upon matrix theory and can be applied to get the estimated low rank matrix and the estimated sparse matrix from the corrupted observation matrix. Once the low rank and

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

sparse matrices are estimated, the received signal power can be estimated for the suspect nodes. This transmission energy data is removed from the collected data at the fusion center. The data cache is no longer poisoned, and the determination of the presence of a primary user is more accurate.

The authors of [23,108] provide methods of determining if a primary user emulator is in the network when the primary user location is known and fixed. The method of the paper [23] is based on using a trust based transmitter verification scheme to properly vet the primary user. It is assumed all radios are aware of the location of, and therefore the distance to, the primary users in the area. The distance between the primary user and the cognitive radio is calculated based on known coordinates. The distance between radio and the user sending the primary user type signal is also calculated based on the received power levels. The trustworthiness of the user is determined by a comparison of the resulting distances. Fig. 1 reflects the flow of the decision process.

In [108] the authors provide a method of defense against the primary user emulation attack using belief propagation. All secondary users in the network iteratively calculate the location function, a compatibility function, compute messages, exchange the messages with neighbors, and calculate the belief function until convergence. At convergence, any existing attacker will be detected, and secondary users will be notified of the attacker's signal characteristics via broadcast message. This allows all secondary users to avoid the attacker's primary emulation signal in the future.

The location function can locate the attacker based on differences in the received strength of the transmitted signal. Since none of the secondary users are aware of the transmitted signal strength or their distance from the attacker, the pinpointing of the attacker location depends upon the difference in measured signal strength by several neighbors. It was determined that one secondary node needs to interact with at least three neighboring nodes to estimate the attacker's location. After determining the location and computing the compatibility function until convergence, if the belief manipulation sum is higher than a specific threshold, the transmitter is determined to be the primary user, and not an attacker.

Similarly, the authors of [16] describe a transmitter verification scheme called LocDef (localization based defense). The scheme verifies whether a signal is from an incumbent by estimating its location and observing the signal fingerprint. Localization is determined by utilizing an underlying wireless sensor network. The underlying network collects snapshots of received signal strength across the cognitive radio network. The collected measurements are smoothed and the peaks are identified. Using the peaks, the transmitter locations can be identified.

The papers [15,28] propose methods for cooperative sensing in the presence of a primary user emulator and the probable detection of a primary user. When an attack is underway, secondary users in the area receive the signals from both primary user and attacker. This sensing information is sent to the fusion center. In [28], when differing signal energy is reported as determined by a network

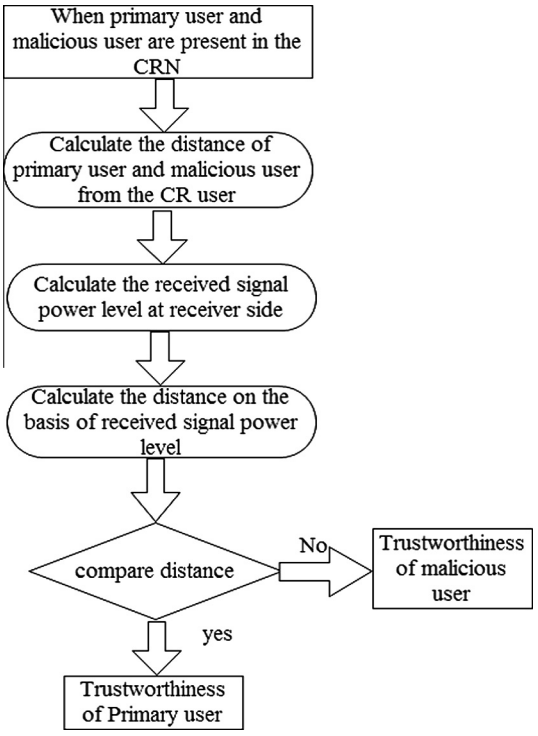

Fig. 1. Proposed transmitter verification scheme [23].

threshold, statistical probability is applied to the reports to determine if the primary user or a malicious emulator is present.

In [15] the information is combined with a weighting system to maximize the probability of detection within the constraints of a false alarm probability. The weights are related to the channel state information (CSI) between the nodes. The CSI is estimated using existing channel estimation algorithms. The method presented maximizes the probability of detection of the primary user by deriving optimal weights. It must be noted that the paper [15] assumes the primary user emulator (attacker) has been determined as present, so the goal is to detect the primary user in the presence of the attacker with the assistance of multiple cooperative cognitive radio users.

Identification of a primary user emulator through a radio fingerprint has been proposed in the papers [17,30,99,114]. With a radio fingerprint, a wireless device can be identified by its unique transmission characteristics. Electronic fingerprinting is already used by cellular operators to prevent cell phone cloning. The fingerprint is due to the slight variations in the manufacture of the hardware components.

In the paper [17], the authors employ the spectrum sensing capability of the cognitive radio itself to identify primary user attacks. The uniqueness, or fingerprint, of the wireless signals is determined by use of the Neyman–Pearson test. The test is used to differentiate between the channel states of transmitters over Rayleigh fading channels. Simulation showed the method was effective in identifying a primary user emulator, thereby allowing the network to defend against the attack.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

The authors of [114] focus on the phase noise of a signal created by the local oscillator. Phase noise is the rapid, random fluctuations in the phase of the waveform. It causes spectrum spread and deformation, and is unique. After extraction of the phase noise from the received modulated signal, applet wavelet and higher order statistical analysis is applied to identify the fake primary user transmitters. Results of simulation experiments showed the phase noise of two receivers using the same local oscillators was different. This indicates it is feasible to identify a transmitter for primary user emulation defense.

Performance analysis of the cognitive radio network is the focus of the paper [110]. The authors create a three dimensional Markov model to provide a method of performance analysis using a common control channel when under primary user attack. The outage probability metric is redefined, and the new performance metric common control channel recovery time is introduced. Together, the metrics identify and evaluate the impact of the common control channel on the network. The blocking rate and dropping rate of the cognitive radio network are also calculated.

Outage probability, or the probability of network suspension, reflects the chance a cognitive radio network will suspend. Suspension occurs with the arrival of a new primary user when all of the available N channels are already being utilized by only primary users (PU), fake primary users (fPU), and the common control channel. Since no secondary users (SU) are currently using a channel, the common control channel must drop, opening the frequency for the new primary user. At this point the cognitive radio network is suspended.

With the system state defined as (i, j, k) where i and j represent the number of primary users and primary user emulators, and k represents the sum of the secondary users plus the common control channel, the outage probability is the sum of the state probabilities where $k = 0$. Therefore, the outage probability is determined by

$$P_{outage} = \sum_{(i,j,k)\in\Omega} P_{(i,j,k)} \tag{1}$$

where $\Omega = \{(i,j,k)/(i + j) = N \text{ and } k = 0\}$.

The common control channel recovery time is the average time expected for recovery after an outage. The common control channel will only recover by using a channel vacated by a primary user or primary user emulator. The analysis is based upon the property that the sum of two Poisson processes results in a Poisson process. Therefore, the state probability distribution combined with the holding time of the local primary users and emulators provides the common control channel recovery time as

$$T_{CCC} = \sum_{(i,j,k)\in\Omega_2} \frac{1}{i\mu_{PU} + j\mu_{PU} + \lambda\mu_{PU}} P_{(i,j,k)} + \frac{1}{N\mu_{PU}} P_{(N,0,0)}, \tag{2}$$

where $\Omega_2 = \{i + j = N,\ j > 0,\ k = 0\}$, the arrival rates of PUs, fake PUs and SUs are λ_{PU}, λ_{fPU} and λ_{SU}, respectively, and the channel holding times exponentially distributed with the mean are $\frac{1}{\mu_{PU}}$, $\frac{1}{\mu_{fPU}}$, and $\frac{1}{\mu_{SU}}$.

As expected, the analysis of tests using the formulas above show that a network under the attack of primary user emulators takes a longer time to recover than a network not under attack. This recovery time was also shown to increase as the number of primary user emulators increased. Additionally, the larger the number of primary user emulators, the greater chance the network would drop into the suspended state.

3.2. Objective function attack

Cognitive radios are adaptive to the environment. Many radio parameters are available for manipulation in the effort to adapt the radio to the environment by maximizing objective functions, and therefore the radio's ability to communicate over the medium. Objective function attacks apply to an attack on any learning algorithms that utilize objective functions. Another name for objective function attacks is belief manipulation attacks. Parameters manipulated include, but are not limited to, bandwidth, power, modulation, coding rate, frequency, frame size, encryption type, and channel access protocol.

The authors of [18] give the following objective function example. Assume the function exists where w_i are weights, P is power, R is rate, and S is security.

$$f = w_1P + w_2R + w_3S \tag{3}$$

Now assume an attacker wishes to lower the security with which the radio is transmitting messages. The attacker would monitor the channel, and jam the channel whenever the radio tries to send a message at the more secure level. The cognitive radio would learn that attempting to transmit at the higher security level would not be successful. This would result in either the higher security messages being sent at a lower security level, or the messages would not be sent at all. Similar attacks could cause a radio to avoid certain frequencies, rates, modulations, or bandwidths.

There have been few clearly effective methods of mitigating objective function attacks. One simple proposal has been made by [44]. The proposal suggests naively defining thresholds for each of the adjustable parameters. Communication would be prevented when one or more of the parameters did not fulfill its predefined threshold.

The authors of the papers [13,106] present the covert adaptive injection attack. In these examples of an objective function attack, the attacker is capable of learning and adjusting its strategies in response to the environment. The attacker attempts to stealthily manipulate the sensing results of a distributed network, thereby attacking the objective functions and decision making of the cognitive radio network. A robust distributed outlier detection scheme is presented to counter the covert attack.

The method presented by [106] uses a localized detection threshold at each node, and adapts the threshold with the diminishing behavior of state differences, exploiting the state convergence property. With this scheme, it is more difficult for an attacker to guess all of the thresholds of the neighbors at any instance. When a network node suspects an attacker, it sends a primitive alarm to its immediate neighbors. The alarm is not forwarded. If the node collects primitive alarms from at least half of the nodes that are common neighbors of the node and

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

suspected attacker, it broadcasts a confirmed alarm. The confirmed alarm is forwarded to the remaining network. Verification of the attacker is provided using a hash based computation. This verification ensures the correctness of a neighbor's state update process with the goal of thwarting collusion attacks by common neighbor cross validation.

Rather than using a threshold and alarms, the method presented in [13] uses a neighborhood voting system. After each secondary user has collected the sensing reports from its immediate neighbors, the nodes determine an algorithm based mean, and conduct a spatial correlation test. Based on the results, each node casts votes about the legitimacy of each of its neighbors. If a node receives more than half of the neighbor votes categorizing it as suspicious, the node is considered malicious.

The authors of [81] present a solution to the false channel information exchange attack. This is a form of the objective function attack because the goal of the attacker is to affect the decision making algorithms of the network nodes. The authenticity of the received channel information is analyzed using spatial correlation algorithms. Simulation shows that the algorithms achieve a high detection rate of malicious nodes with a low false alarm rate.

In [103] the authors explore a framework of power control schemes based on a robust Markov decision process. If an attacker can influence the power scheme of the radio, the attacker can affect the throughput of the network. Additionally, the authors use a delayed Markov decision process to model the throughput maximization problem while experiencing spectrum sensing delay caused by a malicious user. The delayed Markov decision process is solved by using a modified dynamic programming approach.

Belief manipulation attacks as related to the knowledge base of learning algorithms is presented in [5]. Many defense methods have been studied as related to the mitigation of jamming and other throughput affecting attacks. However, less studied has been the effect on the learning that takes place over time based on the objective function results, and how the learning is poisoned by intermittent attacks. To determine if there is an attacker present, monitor nodes are assigned to sample the channels over a time window and Wald's Sequential Probability Ratio Test rule is applied.

The softmax policy [85] includes randomized user actions based on some probability distribution in an effort to hide information about the learning algorithm. In the algorithm, more weight is applied to actions that performed well in the past. By avoiding the attacker's influence by using and sensing channels where the attacker is not expected to be present, the learning algorithm is reinforced and becomes increasingly accurate.

3.3. Overlapping secondary user

As shown in Fig. 2, a geographical region may contain coexisting, overlapping multiple secondary networks. Such a situation places dynamic spectrum access sharing at risk through both objective function and primary user vulnerabilities by one malicious node, or accidentally by a friendly node. A malicious user in one network may transmit signals that cause harm to the primary and secondary users of both networks. Signals transmitted maliciously may provide false sensing information, thereby negatively affecting the objective function in one or both networks. The malicious user may intermittently falsely emulate the primary users of each network causing each network to vacate the channel. Additionally, in special situations a friendly node reporting the presence of the primary user in Network 1 may inadvertently be relaying the same information to Network 2, negatively impacting Network 2's objective function.

This attack can be especially hard to prevent since the malicious node may not be under the direct control of the secondary station or users of the victim network. This is essentially an attack on the capability of the cognitive radio network for spectrum sensing and sharing of both infrastructure and ad hoc based networks. The result is a denial of service attack.

The authors of [109] provide three possible mitigation solution categories for the overlapping secondary user attack. These mitigation techniques are also applicable to many other denial of service attacks, and are based upon work in other areas.

1. *Modifying the modulation scheme:* The use of frequency hopping and direct sequence spread spectrum techniques can make it more difficult to launch effective denial of service attacks. The attacks may still degrade service quality.
2. *Detection and prevention of attacks:* Observing the primary user's location and signal characteristics, as described in Section 3.1, "Primary User Emulator Attack", can help the network identify if a node is performing maliciously.
3. *Using authentication and trust models:* In the paper [97] a system is designed to determine a suspicion level, trust value, and consistency value to identify and exclude a malicious user. Nodes become suspicious when the reported channel state is not in agreement with the channel state reported by others. A trust value for each node is calculated over time, and a consistency value reflects the consistent trust value over time. A node with a consistently low trust value will eventually be identified as a possible malicious user and dropped from the network.

3.4. Jamming

Cognitive radio networks require a minimum signal to noise ratio to decode a signal sent from their corresponding transceivers. Jamming, one of the most basic types of attacks in the cognitive radio network, attempts to adversely affect the signal to noise ratio. In this attack, the malicious user intentionally and continuously transmits on a licensed band, making it unusable by the primary or other secondary users. The attack is amplified by transmitting with high power in several spectral bands. Jamming can be detected with triangulation and energy based techniques. However, the time lost with these techniques allows the attacker to severely impact the network. A mobile attacker can be even more difficult to locate.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

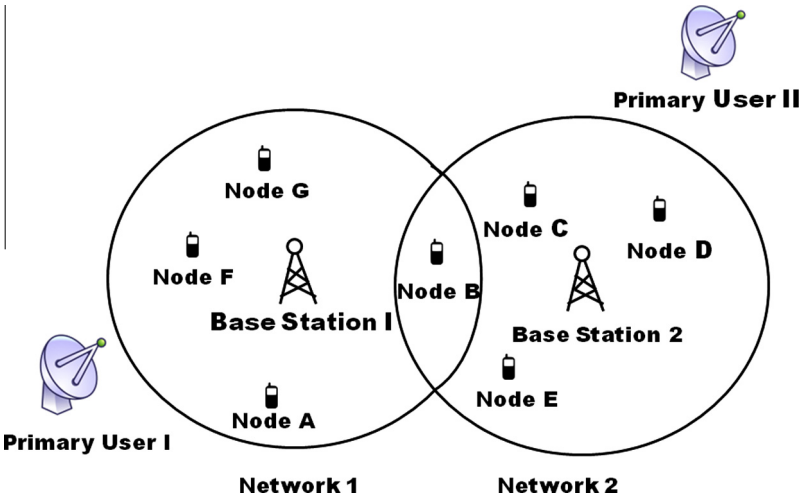

Fig. 2. Overlapping secondary attack.

Before initiating mitigation techniques against jamming, the cognitive radio network must first determine that a jammer exists. Besides the presence and actions of a jammer, poor performance experienced by a receiving node can also be caused by natural causes such as network congestion.

A statistical approach is often used for detecting anomalous spectrum usage attacks, specifically stealthy jamming, and is proposed in both papers [71,82]. In [71], the statistical analysis is a three step cross-layer process. First, statistical analysis is performed on the information gathered from multiple layers. Next, a multiple layer discrepancy search is conducted on the data collected by comparing the data from several layers. In the third step, simple statistical measures are used to determine if there are discrepancies among the data from the network and physical layers using only snapshot data. For instance, the physical layer may report numerous available channels in the area, but few nodes appear in the resultant paths. This may indicate jamming is occurring. Due to the possibility that there can be other reasons the nodes do not appear, there could be a high false alarm rate if a comparison to historic data is not conducted.

Using time series data available from multiple layers can minimize the false alarm probability. This is because the probability distribution of chosen observables will change when the network is under attack. The observables are carefully chosen such that their statistics will indicate a sharp change with high probability in the presence of an attacker. Although it is assumed the data from different layers is independent, it has been shown that the observed changes before and after the event are related via time.

In the paper [82] sequential detection is used to compare the statistical distribution before and after an attack. Confirmation of attack is obtained by a cross-layer three step process. First, the statistical analysis of the paths/nodes is obtained from route discovery. If there are anomalous patterns observed, passive checking is performed by cross checking the pattern with the physical layer spectrum sensing results. Last, active checking is performed by selectively injecting controlled traffic into the potentially congested area and collecting measurements. The passive and active steps are conducted to confirm the results in the statistical analysis.

Jamming is an attack that affects both cooperative and uncooperative cognitive radio networks. In general, uncooperative networks are more resistant to jamming attacks because the nodes do not need to use a common channel to share information about the frequency to which they are hopping. In cooperative networks, the jammer can either capture the shared channel information and move to the same frequency to continue the attack, or inhibit the channel data exchange by jamming the common channel. However, although existing anti-jamming schemes for uncooperative networks are more robust when under attack, they are not as efficient as cooperative network channel sharing schemes when not under attack [83]. With no jammer present, network throughput is lower in uncooperative networks because the nodes need to use energy in the attempt to discover upon which channel the intended transmitter/receiver is transmitting/listening. Therefore, combining cooperative frequency sharing techniques with uncooperative networking and anti-jamming methods will make the cognitive radio network adaptable to changing network conditions while preserving network throughput. Below we describe anti-jamming methods for both cooperative and uncooperative networks.

3.4.1. Cooperative network jamming mitigation techniques

A scenario comprised of a primary user, secondary user, and jammer was studied in the paper [10]. The authors conducted a simulated jamming attack to derive the best combinations of the number of control and data channels to enhance the legitimate secondary user transmission during jamming. The data and control channel allocation determination was also specific to the type of application and the quality of service required for good throughput of the application. It was shown that there is a tradeoff between efficiency and transmission probability when allocating more than one channel to common control.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

Additionally, it was noted that the results did not always conform to what was initially expected. For an example, using the extremely conservative strategy of five control channels and three data channels was less efficient than using a less conservative strategy of four control channels and four data channels for an electronic mail application under jamming attack.

The paper [96] explores collaborative defense of the network against collaborative jammers. The collaborative defense is mounted using a multi-tier proxy based cooperative defense strategy designed to exploit the temporal and spatial diversity available to the legitimate users in an infrastructure based cognitive radio network. The network is divided between proxies and followers. The proxies act as relays between the followers and the base station. Followers must connect to a proxy, rather than straight to the base station. This adds another layer to the communication hierarchy. When the users cooperate, the jammers necessarily need to jam both the followers and proxies to jam all communication. Therefore, with the collaborative defense strategy, the jammers need more jammers to effectively suspend the network communication. Simulation results show that spectrum availability is greatly improved when the users cooperate. However, due to the extra layer in the communication hierarchy, the latency of communication is also increased.

A targeted jamming attack and its mitigation is presented in [33]. The authors describe the "Most Active Band" attack in which a jammer determines and targets the band with the most traffic for jamming, resulting in denial of service on that band. The coordinated concealment strategy (CCS) is offered as a countermeasure. Basically, a few secondary user nodes sacrifice themselves by moving to a single band, drawing the attacker's attention. The "surviving" nodes are free to operate on other bands under the concealment of the ruse.

In [79,93] the authors assume the jammer's signal and the primary user signal are distinguishable and the attackers will not jam the primary user. The contention between the jammer and the secondary users is based upon the secondary users' aim at maximizing spectrum utilization with carefully designed channel switching schedules, while the malicious attacker's desire is to decrease spectrum utilization by strategic jamming. From this description, the objectives of the secondary user and jammer are opposite, and can be modeled as a zero sum game. In the game model the secondary users adapt their strategy on switching between control and data channels according to their observations about spectrum availability, channel quality, and attacker's actions. According to simulation the calculated optimal policy can achieve better performance in terms of throughput as compared to a learning policy that only maximizes the payoff at each stage while not considering the environment's dynamics, the attackers' cognitive capability, and a random defense policy.

A game theoretic perspective is also used to determine the optimal defense strategy in [111]. A simple stochastic swarm optimization algorithm, called particle swarm optimization (PSO), is applied to solve the optimization problems numerically. PSO is motivated by many natural phenomena, and has been shown to represent each group member seeking the optimal solution for itself as it relates to its neighbors.

3.4.2. Uncooperative network jamming mitigation techniques

The authors of [19] provide a jamming solution based on a distributed, probabilistic protocol. This method is unique in that it avoids control channels, does not require information related to the node neighborhood, and does not require statistics about the channel usage. Instead, the solution is based upon probabilistic pairing approach that allows the node to dynamically find a peer and sync on a random, available frequency. The solution also requires the nodes be preloaded with pairwise keys which are used as seeds to the process of finding a common frequency band. In the syncing process, each node randomly chooses a key and challenges its neighbors. If there is a collision, the nodes agree on a frequency band for communication. Nodes experiencing no collision again randomly choose a key and challenge their neighbors. For the scheme to work, each node needs to dynamically sense the spectrum to determine a frequency free for use.

The authors of [101] developed a channel hopping defense strategy using the Markov decision process approach based on a secondary user that uses only one channel. To adequately use the decision process the user must learn some attacker information by observing the environment. The secondary user first estimates useful parameters based on past observations using maximum likelihood estimation (MLE). The user then utilizes the Q-learning process, which is presented as an avenue for the secondary user to learn and update the defense strategy without knowledge of the underlying Markov model. The scenario is extended such that the secondary user can utilize all available channels simultaneously. In this scenario, randomized power allocation is used as the defense strategy. Derivation of the Nash equilibrium for this Colonel Blotto game provides minimization of the worst-case damage.

In the paper [14], the authors developed a similar jamming hopping, policy iteration scheme based on the Markov Decision Process which utilizes the Q-learning process to lessen the computation burden. However, in this scheme the secondary user has a finite set of channels from which to choose. The set of channel choices is dependent upon the state of the environment at decision time.

The paper [26] uses a game theoretic context to formulate the interaction between communicating nodes and an adversary. Experimental results show that randomized actions by both the secondary user and the jammer result in lower game values than the expected Nash equilibrium for pure information centric channel capacity. Results also show that packetized, adaptive communication is an advantage for the power limited jammer. Additionally, it is proven there exists a threshold on the average power of a jammer above which the transmitter must use a rate equivalent to the maximum power of the jammer.

The authors of the paper [80] present the solution to jamming modeled after a solution to a multi-armed bandit problem. In this scenario the secondary user is the player trying to pull the most rewarding lever at each time slot. The authors use Whittle's linear program to determine

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

which channel the secondary user should select for transmission. The model is valid for a situation in which the state of the non-accessed channels changes when not chosen. For the situation in which the state of the channels is static even when not chosen (in other words, the jammer's strategy is fixed), the author's solution is based on a stochastic multi-armed bandit process using indexing solutions.

Similarly, the authors of [94,95] formulate the jamming problem as a multi-armed bandit problem. In this solution the secondary sender and the receiver both adaptively choose their sending and receiving channels by basing their decisions on all of their past decisions and observations. With the convergence of the learning algorithms, the sender and receiver hop to the same set of channels with high probability under the presence of a jammer.

The paper [83] presents the Uncoordinated Frequency Hopping (UFH) scheme in an effort to allow key establishment between two nodes in the presence of a jammer without a pre-shared key. With the assumption that a jammer cannot jam all of the communication channels at the same time, the message is divided into multiple parts and sent across several frequencies according to a random frequency hopping scheme. Although a secret channel sequence is not utilized by the sender and receiver, it is shown that with sufficient transmission attempts the sender and receiver will converge upon the same channels in a number of time slots. Note also that the time slots for the sender and receiver do not need to be synchronized; instead the receiver is allowed to switch channels less often than the sender. The effect is a reduced number of partially received fragments. Experimental results show that the UFH scheme achieves the same level of anti-jamming protection as coordinated frequency hopping. However, the experiments also show that the UFH scheme results in lower communication throughput with higher storage and processing costs.

The authors of [48] present the time delayed broadcast scheme (TDBS). The scheme does not rely upon commonly shared secrets or common control channels to coordinate broadcasts. Alternately, the scheme relies upon a pseudo-noise (PN) frequency hopping sequence to establish communication. Unlike conventional PN sequences for multi-access systems, the PN sequence presented exhibits high correlation to enable broadcast. Additionally, the experimental results show the TDBS scheme can support and maintain broadcast communications while in the presence of an inside jammer.

The paper [61] examines the resiliency of rate adaptation algorithms (RAA) against smart jamming attacks. According to the experimental results, several techniques can prevent smart jamming by limiting the amount of key information that can be inferred by an attacker. The lack of information forces the attacker to operate as a memory-less jammer. For example, the SampleRate protocol can be protected by using randomized, non-sequential probing. To conceal the explicit and implicit rate information, such information should be protected using post-coding encryption. Using a shared secret key and a random initialization vector can ensure the explicit and implicit rate information is concealed.

In the work [11] the authors present another secret sharing mechanism that does not require pre-shared secret keys. The method is called Time Reversed Message Extraction and Key Scheduling (TREKS). The TREKS mechanism is shown to be efficient and adversary resilient and is based upon intractable forward decoding and efficient backdoor decoding. As with the other methods provided which do not use pre-shared secret keys, TREKS solves the circular dependency problem. Additionally, experimentation showed that TREKS was four magnitudes faster than the prior solutions to CDP, with minimum storage overhead and at most twice the computation required for traditional spread spectrum communication.

4. Media access control layer

The Media Access Control (MAC) layer is a sublayer of the data link layer. The MAC layer is designed to support multiple users on a shared medium within the same network. A Common Control Channel (CCC) may be used for an exchange of control messages to coordinate the users.

4.1. Byzantine attack

In the Byzantine attack, also known as spectrum sensing data falsification, the attacker injecting the false sensing information into the decision stream is a legitimate member of the network and is referred to as the Byzantine. Byzantines may perpetrate the attack to selfishly acquire increased spectrum availability for themselves, or the attackers may have a goal of disrupting the throughput of the network for other nefarious reasons.

The authors of [88] propose a method of detection of Byzantines called Pinokio. Pinokio uses a Misbehavior Detection System (MDS) that maintains a profile of the network's normal behavior based on training data. The MDS detects misbehavior by monitoring the bit rate behavior. By protocol, the bit rate should change periodically and be adjusted by a node contiguously, the bit rates between two nodes should show some reciprocity, and the usage of a low bit rate should occur over a narrow channel. Nodes not exhibiting these characteristics are not acting in a manner conducive to spectrum efficiency, and so are suspect.

Another method of misbehavior detection called Cooperative neighboring cognitive radio nodes (COOPON) is provided by the authors of [38]. Detection of the selfish node is detected by the cooperation of other legitimate neighboring nodes. All of the secondary nodes exchange channel allocation information both received and sent to the suspect nodes. Each neighbor compares the number of channels reported to be used by the suspect node to the channels the neighbors report as being used. A discrepancy reveals a selfish actor.

Several techniques have been proposed related to trust and reputation metrics. In the context of cognitive radio networks, trust and reputation based schemes are very similar. Trust in a behavior based model is defined as the mutual relationship between two entities for a specific action. Trust most often refers to acknowledging nodes

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

that are proven trustworthy in some way. Alternatively, reputation schemes are generally more interested in identifying those nodes that are bad actors.

A trust framework is proposed by [56] consisting of a TrustPolicy Engine and a TrustMetrics Engine. The TrustPolicy Engine targets four main areas: security mechanisms, enhancing secondary user's worthiness, spectrum sharing with legacy networks, and inter-operator spectrum sharing. The engine is designed to analyze the behavior of a cognitive radio according to the notion of trustworthiness. The proposed solution considers two types of trust. Social trust is based on historical actions; quality of service trust is related to performance issues. Both trust aspects are used to determine a trust level based on past behavior and impact on the performance of the network.

The TrustMetrics Engine provides for the exchange of trust information between the nodes and algorithms. This information consists of past performance actions and impacts, and is used to create a prediction of future behaviors. The data is passed to a Performance Engine that implements mechanisms to thwart cognitive radio network attacks.

Several recent authors have tackled the idea of trust or reputation based mitigation methods for the Byzantine attack using the sensed data sent to the fusion center. The authors analyze the case in which the Byzantines do not send true information about the state of spectrum. The information sent by the suspect nodes is compared to the information received from a trusted node.

In the paper [25], a node's reported sensed data that deviates from the data supplied by a trusted source results in the node being labeled as malicious. In [60], when differing signal energy is reported as determined by a network threshold, statistical probability is applied to the reports to determine if a malicious node is present.

The papers [21,46,73,104] all use reputation based detection schemes over time to identify bad actors. In these schemes, a reputation measure is assigned to each node representing the number of times the local decision of a node was different than the global decision of the fusion center in a time window. The higher the value of the measure, the less reliable the node's observation is considered. To increase the accuracy of the decisions made by the fusion center, data from nodes with a high number of mismatches is not included in the sensing algorithms. The papers differ in the algorithms, weights, and observables used to determine the trust levels of the nodes.

In [62,65,66] the authors present trust based authentication systems. In the model in the paper [62], the node with the highest level of trust is appointed as the base station. Authentication between each node and the base is accomplished in two ways. With cryptographic authentication, the base station generates secret keys for the network members. Each node shares a unique key with the base station.

With the certificate based trust authentication technique, the base station generates trust values for each node. Trust values are based upon the recent activities of a node in the network, such as success or failure in forwarding a packet, and the length of time the node has been a member of the network. The trust value of each node is updated by the base station every time the base station sends a broadcast message. If a request is received by the base station, the base station references the node's trust value for a determination of the appropriate action. A second secret key is shared between the base and all nodes of a specific, equal trust level.

The base station also sets a trust threshold for the network. Any node not meeting the minimum trust threshold is expelled from the network and placed on a blacklist for rejection of future joining or other requests. By using the trust method, any bad actors, or Byzantines, in the network will be identified and segregated from the network.

The method to assign trust in [66] is based on three factors for determining sensing trust level. Context is the first factor and includes time, location, spectrum, code, and angle. The second factor is based on sensing evidence scope and importance. This factor reflects the importance of evidence based on the impact of the action on the network. Lastly, all node behavior is collected relative to a time window. The time window allows a node fluctuating between trustworthy/untrustworthy and considerate/inconsiderate behavior to be properly analyzed for intent over time. Together the three factors help capture the transition of a benevolent, well-behaving node to a malevolent node over time, allowing the network to properly and continuously identify currently misbehaving nodes. Additionally, the algorithm allows the node's reputation to rise slowly but fall quickly to punish a secondary user's erratic behavior. The reputation values are considered in data fusion and resource allocation for the secondary users.

The trust calculation presented in [65] relies on several steps and inputs. The direct trust calculation is based on a cumulative attribute determined by the success or failure of past requests, responses, and retransmissions. The indirect trust calculation considers the neighbors' determination of the node's trust. The trust values are integrated, and a historical trust value is added to the algorithm. The node's ability to access the network resources is based upon the trust determination.

The unfair penalization of honest users due to severe pathloss in some locations is considered in the trust based scheme proposed by [35]. The proposed Location Reliability and Malicious Intention (LRMI) trust metric has two parts:

1. Location Reliability reflects pathloss characteristics of the wireless channel.
2. Malicious Intention captures the true intention of secondary users.

Evaluation of sensing reports sent to the fusion center is based on two sources of evidence—the cell the report was sent from (Location Reliability) and who generated the report (Malicious Intention). A trust value is applied to each cell based on the activity of the cell members. The Dempster–Shafer theory is used to evaluate trustworthiness as related to a mobile node. The algorithmic combination of the two values help to alleviate the trust devaluation that generally occurs due to a node's signal pathloss because of its location and mobility, hence providing a more accurate trust determination.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

In the paper [31] the authors present an alternate detection method using two conditional frequency check statistics (CFC). The statistics are developed under the Markovian model for the spectrum state and are not adversely affected by an increasing number of Byzantines. The newly proposed CFC enforces two constraints on the attacker's behavior as compared to the conventional one constraint. This is done by exploring the correlation between the consecutive spectrum states.

The fusion center evaluates the two CFCs for every sensor and compares the results to those of a trusted sensor. Differing values between a sensor and the trusted sensor indicate the corresponding sensor is malicious. Consequently, any flipping attacker that maliciously flips its local inference can easily be identified with the CFC. With at least one trusted user the method can achieve an accuracy rate of greater than 94% in detecting malicious users.

Statistically based analysis schemes that detect malicious users and alleviate the false sensing observations are proposed in [3,39]. The first scheme, proposed by [3], allows for an unknown number of malicious cognitive radios in a network, with the possibility that any node can suddenly turn malicious. The mathematical basis for sensed data analysis is a modified version of the Grubb's test for the detection of a single outlier in a normally distributed data set. Simulations showed that the modified Grubb's test was able to detect any number of malicious cognitive radios in a network, as long as at least half of the network was made up of trustworthy nodes. The second paper [39] compares the Dixon's test for outliers, the Grubb's test for outliers, and the box plot test when applied to sensed data. It is shown that the Dixon's test out performs the Grubb's test and the box plot test in detecting the presence of a single bad actor.

The authors of the paper [67] use a statistical attack model to aid in the development of a Bayesian approach to identifying malicious nodes. Belief propagation is used with factor graphs to solve the Bayesian estimation problem and the derivation of an algorithm. The algorithm is used to estimate channel status and the attack probabilities of the malicious nodes, thereby identifying the Byzantines.

A technique using the primary user's received signal strength (RSS) is introduced in [105]. The method has been shown to work no matter the ratio of trustworthy nodes to malicious nodes in the network. The technique compares the location determined by the strength of the primary user's received signal at a secondary user and reported to the fusion center, to that calculated using the combined data from the network secondary users at the fusion center. This comparison is used to determine whether the secondary user node is providing true or false data.

The authors of [22] present a punishment based mitigation scheme. Using the indirect punishment method, the malicious user does not need to be identified. There only needs to occur collisions with the primary user. It is assumed that when such a collision occurs, the primary user applies a punishment to the entire network. If the attacker can be determined, a punishment is applied directly. Assuming the bad actor is acting selfishly, either punishment will deny the malicious node throughput over the network, and will cause the node to change its behavior.

Alternatively, the authors of [8] present an incentive, or payment based solution that makes it detrimental to a node to refuse to forward packets over free channels. The basis of the system is that a node will receive payment after offering a free channel to forward packets for a neighbor. A transmitting node will pay a neighbor for packet transmission over a channel when that neighbor's services are required for transmission. A central authority is required to maintain the credit balance for each node.

4.2. Control channel saturation

The control channel saturation attack is based on the fact that if a cognitive radio is unable to complete negotiations during the limited time of the control phase, the radio defers from transmission during the next data phase. This situation may naturally occur when the channel is saturated by a large number of contending cognitive radios. An attacker can broadcast a large number of packets with the intent to saturate the control channel. By sending different types of packets, a malicious node reduces the risk of detection. Combining the control channel saturation attack with the small window backoff attack (described in Section 8.2 "Small Backoff Window"), the attacker may be able to ensure the malicious node captures the control channel before other users.

The authors of [52] propose using dynamic channelization to address the common control channel access problem. The authors define an atomic channel as a basic unit of b Hz. Upon the event of control channel migration, a composite channel is formed from the atomic channels, centered around a new carrier frequency. The formula $f = f_0 + mb$ provides for the shifting of the center of frequency from f_0 to f by a multiple of the basic unit b Hz where $m = 0, \pm1, \pm2$, etc. The bandwidth around f can be obtained by channelization as a factor of kb, such that $k = 1, 3, 5$, etc. Fig. 3 shows the migrated control channel for the case of $(m, k) = (4, 3)$.

The paper [59] presents a method to react to control channel saturation with an alternative decision making strategy based on rendezvous negotiation to ensure user's communication coordination. In essence, the paper presents a mathematical analysis of the resources required for channel negotiation for the network based upon the number of secondary users present and the current channel throughput. When the common control channel usage approaches the point at which the additional allotment of resources to rendezvous channel negotiation will create a

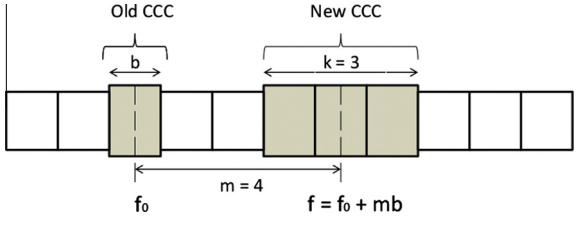

Fig. 3. Migration of common control channel with $(m, k) = (4, 3)$.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

saturation condition, the network moves to the phase of rendezvous channel negotiation. This method avoids the situation in which common channel saturation is reached, and there are no resources available for additional channel rendezvous negotiation. Therefore, the early channel analysis and start of negotiation prevents the waste of data transmission resources while the common control channel is saturated.

4.3. Control channel jamming

Control channels facilitate the cooperation among cognitive radio users. As a single point of failure, common control channel jamming (CCC) is the most effective and energy efficient way for an attacker to destroy the entire network system. With common control channel jamming, receivers are prevented from receiving valid control messages when a strong signal is injected into the control channel. This results in denial of service for users of the network [49].

Using dynamic control channel allocation methods combats control channel jamming by maintaining control communications during the attack. There are two methods for dynamic allocation of control channels: cross channel communication [52] and frequency hopping [42].

The authors of [52] take advantage of the fact that successful communications during a jamming attack can be conducted on another channel not affected by jamming signals. Cognitive radio users can continue to transmit on the channel experiencing interference to notify other network users not experiencing jamming of the new control channel for receiving control messages. This results in successful communication during jamming by using different channels for transmitting and receiving control messages with neighbors. Although communication is maintained, this method incurs high channel switching overhead for radios equipped with a single transceiver.

In the papers [42,48] the authors present methods to mitigate common control channel jamming for cluster based ad hoc networks using hopping sequences. In this case, the cluster head determines the hopping sequences and identifies the operating control channels for the cluster. Due to the nature of the clustering of the network, the network is partitioned into smaller groups. Therefore, when a jamming attack targets a cluster, the affected network area is reduced. The method presented by [48] differs in that no two nodes share the same hopping sequence.

The mitigation tactic presented by [42] hides the control channel location (frequency), and uses key distribution techniques to allow legitimate users to decrypt the control messages encrypted with keyed hash functions. Control messages are repeatedly transmitted on multiple control channels, so compromised nodes would only have partial keys. Consequently the compromised nodes would be unable to jam all of the control channels. Sufficiently large key distribution with message duplication would therefore allow continuation of control information exchange during jamming attacks.

A polynomial based jamming resilient key assignment protocol is presented by [12]. The key space consists of $p * q$ keys, where p is the number of time slots in a period, and q is the number of control channels. The control transmission is sent repeatedly over all of the control channels in each of the time slots in the period. Each node, including the malicious users, is identified by a unique polynomial. The scheme guarantees access of the nodes to the control channel within a certain time period. However, since the key space must be sufficiently large, based on the number of time slots and control channels, it may incur large control retransmission overhead and delay.

A random key distribution scheme was proposed in [86,87] for control channel access under jamming attack. As in [12], the keys are used to hide the control channel allocation in time slots with duplicate transmission on several control channels. The diversity of keys is large, and so it is probable that authorized users hold keys unknown to compromised users. Keys are periodically reused in time slots to limit the key space and corresponding storage overhead. Cryptographic hash functions are used to map the control channel keys to the allocated frequency and time slot for control channel relocation in a reuse period.

The paper [112] provides a method of control channel jamming avoidance without a pre-shared key distribution system. The control data is distributed through cluster heads in the network with each network node belonging to only one cluster. A cognitive radio network with N nodes requires $2\log_2 N$ keys, with each secondary user receiving $\log_2 N$ keys based on a unique binary ID. Each cluster head generates and sends two control signals in every time period i. The functions $F(k_i, i)$ and $F(k_i', i)$ are used by the cluster head to determine the control channels, and are known to the cluster nodes. All nodes, including the jammer, receive their assigned keys. Since no two nodes have a full set of matching keys as relates to each time period, the jammer will be unable to prevent any node from transmitting in at least one time period.

Referring to the example in Table 2, assume a malicious jammer, node 3. The jammer can jam the channel determined with k_1' in period 1, the channel determined with k_2 in period 2, and the channel determined with k_3 in period 3. However, since none of the other nodes have the same three keys in the same time periods as node 3, each will be able to transmit on the assigned control channel in at least one of the three periods.

A stochastic sum game called jamming resilient control channel (JRCC) is presented in [50]. The game models the interchange among the cognitive radio users and the attacker under the impact of the primary user. The game objective is to determine the best control channel allocation strategy to combat jamming using multiagent

Table 2
Key for 8 secondary users with 1 attacker [112].

Node	Unique ID	Key
0	000	$k_1\ k_2\ k_3$
1	100	$k_1\ k_2\ k_3'$
2	010	$k_1\ k_2'\ k_3$
3	001	$k_1'\ k_2\ k_3$
4	101	$k_1'\ k_2\ k_3'$
5	011	$k_1'\ k_2'\ k_3$
6	111	$k_1'\ k_2'\ k_3'$
7	110	$k_1\ k_2'\ k_3'$

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

reinforcement learning (MARL). The optimal control channel is found when the game reaches the Nash equilibrium.

In each stage of the game, each radio selects an action that maps to a set of selected common control channels. The nodes receive their rewards by complying with conditions applied to each common control channel. To facilitate cooperation, each radio broadcasts the control message according to the conditions of the channel. Each node's strategies are updated with the parameters received from its neighbors. If the primary user changes the game state, the radios sense the channels to obtain the new state, and update their parameters, learning rate, and strategy. In this manner, the JRCC algorithm enables cooperation between the nodes with low overhead to facilitate common control allocations while adapting to the primary user and learning rates. Simulation results show that the JRCC algorithm effectively combats jamming in an environment that includes primary user activity.

5. Network layer

The network layer provides the ability to route data packets from a source node on one network to a destination node on another network, while maintaining quality of service. It also performs fragmentation and reassembly of packets, if required. The cognitive radio network shares security issues with the classic wireless communication networks due to the three shared architectures of mesh, ad hoc, and infrastructure. Cognitive radio networks also share similarities with wireless sensor networks. These include multi-hop routing protocols and power constraints. In addition, there are special challenges faced by cognitive radio networks due to the required transparency of the network activities to the primary user. Routing in the cognitive radio network is further complicated by the requirement of the radio to vacate the frequency when the primary user is sensed as present. Cognitive radio security vulnerabilities are therefore also inherited from these architectural requirements.

5.1. Sinkhole

Cognitive radio networks often use multi-hop routing. A sinkhole attacker takes advantage of multi-hop routing by advertising itself as the best route to a specific destination. This activity spurs neighboring nodes to use it for packet forwarding. In addition, the neighbors of the attacker will advertise the offender as the best route, creating a "sphere of influence" for the attacker.

The attacker can begin the attack by building a trust base. The attacker can use a higher level of power so it can send any received packets directly to the base station. It can advertise that it is one hop from the base station, and forward all received packets appropriately for a time. After trust has been established, and advertising of the node as the best route has been propagated through the local area, the perpetrator can begin other types of attacks, such as eavesdropping.

The attacker can perpetrate the selective forwarding attack by forwarding, dropping, or modifying received packets from select nodes. This attack is particularly effective with mesh and infrastructure architectures since all local traffic looking to be relayed to another network has the same destination; all traffic leaving the local network needs to go through the base station.

Countermeasures for the sinkhole attack from outside the network are based upon link layer authentication and encryption. Using authentication, an outside attacker will be unable to join the network. Since the cognitive radio network will only use members for routing, the attacker will be unable to advertise as the best route [40].

Countermeasures for the insider attack could be based upon a continually updated trust determination. The cognitive radio network would need a system to monitor dropped or changed packets, and report issues to the fusion center. After analyzing the received data, the base station would flood the network notifying its members of the communication issues recently experienced. It would then drop the attacker as a member of the community.

Additionally, countermeasures to the insider attack can be adopted from wireless sensor network studies, such as the security aware ad hoc routing protocol (SAR). SAR is based upon on demand protocols, such as Adhoc On Demand Distance Vector (AODV) routing or Dynamic Source Routing (DSR) [107].

With SAR a security metric is added to the route request packet (RREQ) and the route discovery procedure is modified. Intermediate nodes receiving the RREQ packet determine if the security metric or trust level is satisfied. If it is satisfied, the node processes the packet and uses controlled flooding to propagate the packet. If the required security is not satisfied, the packet is dropped. A reply packet (RREP) is generated if an end to end path can be found based on the required security attributes. A notification is sent to the sender if such a path cannot be found. The sender can then modify the trust level in order to find a route [107,100].

With the assumption that a key cannot be determined by nodes that did not receive it from the base, a malicious node that interrupts the flow by altering the security metric cannot cause serious damage. Without the key, the attacker cannot decrypt the packet, and a legitimate node receiving the packet with an altered security level will drop it [100].

5.2. Wormhole

The wormhole attack is closely related to the sinkhole attack. Basically, an attacker tunnels messages received in one part of the network over a low latency link. The messages are replayed in another part of the network. In the simplest example, a node situated between two other nodes forwards messages between the two of them. Wormhole attacks are usually administered by two malicious nodes that understate the distance between them by relaying packets along an out-of-bound channel that is unavailable to the other nodes.

A wormhole attack is perpetrated by convincing nodes that are usually multiple hops from the base station that they are only one or two hops away through the adversary. If the end point of the wormhole is relatively far from the

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

base station, most nodes in the local network area will try to use the attacker for forwarding. Packets can then be selectively forwarded to the malicious node close to the base station for additional forwarding, or captured for eavesdropping as they are forwarded [34,40] (see Fig. 4).

If the adversaries are placed carefully, the attack could result in a partitioned network when the attackers stop relaying the packets. This action would trigger network routing discovery. Participating in the discovery effort may provide the attacker with additional information that could be used for other attacks, such as eavesdropping.

One prevention method for the wormhole attack was suggested by [40]. Karlof and Wagner suggest using geographic routing protocols to forward packets in the network. Such protocols construct a topology based on routing traffic physically towards the base station. Using this routing method, it is difficult to attract traffic towards a sinkhole or wormhole. Local nodes would detect an artificial link because they would notice the distance between themselves and the attacker, or between the attackers, is beyond normal radio range.

The authors of [34] propose using packet leashes to detect and defend against wormhole attacks. The authors present two types of packet leashes: geographic and temporal. Both leashes allow the receiver of a packet to detect if that packet traveled farther than the leash allows. The geographic leash is used to ensure the packet recipient is within a certain distance from the sender. For the geographical leash to be constructed, each node must be aware of its own location, and the clocks of all nodes must be loosely synchronized. Sending nodes include in their packets their own location and the time the packet was sent. The receiving node compares this data to its own location and the time of receipt. Assuming the clocks of the nodes are loosely synchronized, the receiver can compute an upper bound on the distance between the sender and itself. It is noted that obstacles in the network field would not allow distance bounding based on location data. Therefore, wormholes could still be created, since communication may not be allowed between two nodes that would otherwise be in transmission range.

The temporal leash provides an upper bound on the packet lifetime. This lifetime in effect restricts the maximum travel distance of the packet. Creation of a temporal leash requires tightly synchronized clocks, such that the maximum difference allowed is t. All nodes in the network must be aware of the value of t, and it must be on the order of a few microseconds or less. When sending a packet, the sender would include in the packet the time the packet was sent. The receiving node would compare the time to the time received. From this information, the receiver would be able to determine if the packet had traveled too far based on transmission time and the speed of light.

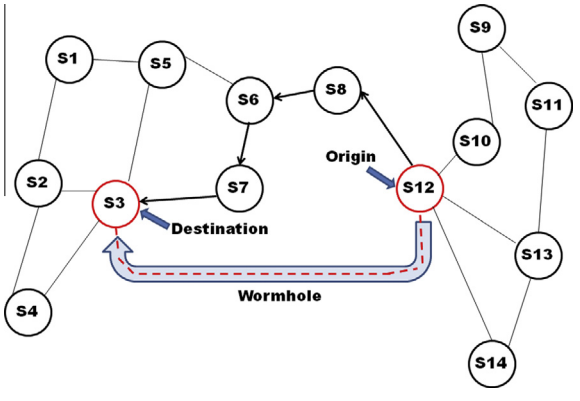

Fig. 4. Wormhole attack.

5.3. HELLO flood

The HELLO attack was first introduced by [40] as an attack against wireless sensor networks. However, due to the possibility of using similar routing strategies, the attack can be applied to the cognitive radio network. The attack is perpetrated by an attacker that broadcasts a message to all nodes in a network. The packet may be advertising a high quality link to a specific destination. Enough power is used to convince each node that the attacking node is their neighbor. The nodes receiving the packets assume the attacker is very close due to the strength of the received signal, when in fact the attacker is a great distance away. Packets sent from the network nodes at the regular signal strength would be lost. In addition, network nodes may find themselves with no neighbors available to forward packets to a particular destination, since all nodes are forwarding packets towards the attacker. Protocols that depend upon localized information exchange between neighbors for topology maintenance are also subject to the attack. Note that an adversary need not to be able to read or construct legitimate traffic; the attacker needs only to capture and rebroadcast overheard packets with enough power to reach every node in the network [40].

The HELLO attack can be defended against by verifying the bi-directionality of links before using the link established by a message received over the same link. Using a base station as a trusted third party to facilitate the establishment of session keys between parties in the network can provide verification of bi-directionality. The session key allows the communicating nodes to verify each other's identity, as well as provides an encrypted link between them. It should be noted the number of shared keys needs to be limited to prevent the attacker from establishing a link between every node. An alarm should be raised about the detection of an attacker if one node claims to be a neighbor to an inordinate number of nodes [24,40].

5.4. Sybil

Local entities that have no direct physical knowledge of remote entities perceive the others as informational abstractions. These are referred to as identities. A system must have the capability to ensure that distinct identities refer to distinct entities [20]. Without this ability, the reputation system used to prevent other types of attacks will be subverted.

An attacker perpetrating the Sybil attack will create a large number of pseudonymous identities so it can gain a

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

disproportionately large influence on the network. In other words, the mapping of identities to entities is many to one. Pairing the Sybil attack with the launch of the primary user and Byzantine attacks can allow the attacker to prevent use of the channel by legitimate users by effectively poisoning the decision making process [89]. Additionally, the misbehavior can be spread amongst the nodes acting as Byzantines, making any one of them especially difficult to identify [58].

Validation of each node's identity is the key to defending against the Sybil attack. The two ways to validate an identity are direct validation, in which a node directly tests whether the identity of another node is valid, and indirect validation, in which nodes that are already verified provide validation or refutation for other nodes.

In [20] resource testing is proposed as a method of direct validation. An assumption made with resource testing is that the resources of the attacker's physical entity are not unlimited. Identities are tested to verify that each identity has as much of a tested resource as a physical device. The authors proposed measuring the resources available for computation, storage, and communication.

One communication testing example is to broadcast a request for identities, and only accept replies that occur within a given time interval. To test storage resources, each entity is asked to store a large amount of unique, incompressible data. The challenging entity keeps small excerpts of the data to use to verify the challenged identities are storing the data they are sent. Finally, to test computation resources, each entity is asked simultaneously to solve a unique puzzle in a limited time.

The authors of [58] suggest another validating method that may be suitable for cognitive radio networks. For the radio resource testing method, it is assumed each physical device has only one radio. It is also assumed that a radio can only send or receive on one channel at any moment. A node can verify that none of its neighbors are Sybil identities by assigning each of the neighbors a different channel on which to broadcast a message. From the same set of channels, a channel is then randomly chosen by the challenger on which to listen. The challenger will hear the message if the neighbor assigned the channel is legitimate.

In [40] a solution involving symmetric keys is suggested. With this solution, every node shares a unique symmetric key with a trusted base station. The base station also acts as a trusted third party to facilitate the establishment of session keys between parties in the network. The session key allows the communicating nodes to verify each other's identity, as well as establish an encrypted link between them. It should be noted the number of shared keys needs to be limited to prevent the attacker from establishing a link between every node. Also, the base station can place a reasonable limit upon the number of neighbors a node is allowed. An alarm should be raised about the detection of an attacker if one node claims to be a neighbor to an inordinate number of nodes.

As mentioned in [104], many of the trust and reputation based schemes previously proposed can be applied to the Sybil problem. Refer to Section 4.1 for descriptions of these techniques. Nodes with a bad reputation, or those that are proven as untrustworthy, will be punished or removed from the network, regardless of whether they are truly a distinct node, or a Sybil.

5.5. Ripple effect

The ripple effect is a new attack that is specific to cognitive radios because of their ability to change channels during communication. Cognitive radios actively change channels to avoid the primary user and to utilize the channel that will provide the best throughput in the local area. The ripple effect is similar to the primary user emulation or Byzantine attack in that the wrong channel information is provided so that the other nodes in the area change their channel. However, the ripple effect attacker's intent is to cause the false information to be passed hop by hop, and in turn cause the network to enter a confused state.

It should be noted that the attack is especially effective when the attacker transmits with a strong signal because of the following:

1. The activity of a primary user is generally greater than that of a secondary user, so the appearance of a primary user may affect several ongoing transmissions of secondary users.
2. Secondary users expend time and energy for spectrum sensing, neighbor discovery, and channel switching (a few milliseconds) when changing channels.
3. Channel switching of one secondary user may cause a ripple effect, or cascaded switching of multiple secondary users [115].

Countermeasures to the ripple effect attack are similar to those for the primary user emulation and Byzantine attacks. It is essential that primary user presence can be detected and validated. Similarly, it is essential that the information passed from a neighbor about the presence of the primary user is also validated. Such validation can ensure the licensed channel is vacated when necessary, and channel switching will only occur when necessary.

6. Transport layer

The transport layer responsibilities include flow control, congestion control, and end-to-end error recovery. The transport layer in the cognitive radio network is subject to many of the vulnerabilities that plague wireless ad hoc networks.

6.1. Key depletion

Cognitive radio networks suffer from short transport layer session duration due to high round trip times and frequently occurring retransmissions [72]. This necessarily implies that a large number of sessions are initiated. Most transport layer protocols, such as secure socket layer (SSL) and transport layer security (TLS), establish cryptographic keys at the beginning of each transport layer session. With the great number of session keys generated, it becomes more likely a session key will be repeated. Repetitions of

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

a key can provide an avenue of exploitation to break the underlying cipher system. It has been established that the wired equivalent privacy (WEP) protocol and temporal key integrity protocol (TKIP) used for IEEE 802.11 are prone to key repetition attacks.

Security protocols used below the network layer currently are designed to accommodate the total number of sessions that are typically created for wireless LANs. The newer Counter Cipher mode with block chaining Message authentication code Protocol (CCMP) is designed to exponentially delay key repetitions [53]. CCMP offers enhanced security compared to TKIP by using 128 bit keys with a 48 bit initialization vector. This architecture minimizes the vulnerability of the system to replay attacks. Since the current design is inadequate for the security requirements of cognitive radio networks, new protocols need to be investigated.

7. Application layer

The application layer is the layer closest to the end user. The user and the application layer interact with the application software. The application layer is responsible for determining the resources available, synchronizing communication, and identifying the communicating devices. Cognitive radios require a greater processing power and memory capacity than the traditional smart phone. This is because of the extra tasks performed by the cognitive radio, such as spectrum sensing and learning. Cognitive radios are therefore expected to be the target of software viruses and malware [4]. Additionally, physical and link layer delays due to spectrum handoffs, unnecessary rerouting and stale routing due to network layer attacks and delays due to frequent key exchanges cause degradation of the QoS in the application layer protocols [53].

7.1. Cognitive radio virus

The cognitive radio network is as vulnerable to viruses as other types of networks and platforms controlled by software. Viruses are computer programs that can replicate themselves and spread from radio to radio. For replication, the virus must be able to execute code and write to memory.

In a self propagating network like the cognitive radio network a virus can be particularly devastating. A radio infected with the virus can impose upon its neighboring node a false state, or a series of transition states. The neighbor will pass along this false state. A particularly troublesome side effect of this propagation is that an artificial intelligence (AI) cognitive radio will erroneously learn to react to this false environment, affecting future network decisions.

The authors of [32] present a model for the propagation of a self propagating AI virus through a cognitive radio network. Simulation showed that the time taken to infect the whole cognitive radio network increased exponentially with network size. Second, it was shown that the antivirus performance of static networks is better than the performance of a dynamic network in the presence of an AI virus. It was also shown that the AI virus propagation speed increases with an available abundant spectrum resource in the area. However, the variability of the spectrum does not affect the propagation speed noticeably.

In the paper [18] the authors suggest a feedback loop into the network to cause the radios to relearn in the case of propagated false environmental information and consequent decisions and learning. A second approach is to build in logic that will invalidate learned actions that are known to violate certain principles.

7.2. Policy attacks

There are four main functions of the policy system of the policy based cognitive radio. They are policy derivation, policy distribution, policy reasoning, and policy enforcement. The paper [6] describes the security threats associated with each of the functions. The attack on the policy derivation and distribution functions by spoofing, and policy reasoning and enforcement threats are described below. The policy attacks via forging occur at a different level targeting the application layer; therefore, those attacks are described under the cross-layer attacks.

The functions of policy derivation and policy distribution can be disrupted by a malicious node through spoofing the policy administrator. With the spoofing attack on policy derivation, the faked policy administrator feeds the radio policy manager false or misleading policies designed to decrease network performance or cause interference with the primary user. Similarly, the spoofing attack on the policy distribution function allows a faked policy server to supply misleading policies to the radio's policy engine. An authentication protocol that uses certificates to validate the policy administrator can mitigate these attacks.

The policy reasoning and enforcement attack occurs when a selfish policy controlled cognitive device sends false reasoned information to other ordinary cognitive controlled devices in the area stating there are no available bands for transmission. In this way the selfish device keeps transmission opportunities for itself. Reputation or collaborative decision schemes are recommended as mitigation avenues.

8. Cross-layer

Cross-layer attacks launched by adversaries target multiple layers. These types of attacks can affect the whole cognitive cycle of spectrum sensing, spectrum analysis, and spectrum decision. Many of the attacks described earlier can be combined to create cross-layer attacks. In addition, the same attacks may target one layer, but affect the performance at another layer. Often the cross-layer attack will take place on the physical layer while targeting the performance of the MAC layer.

8.1. Routing information jamming

This attack can take place in a cognitive network with no common control channel. It also takes advantage of

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

the fact that there is delay during spectrum handoff. The delay allows jamming of the routing information among neighboring nodes. The result is the use of stale routes and incorrect routing of packets.

To start the attack, a malicious node causes the targeted node to initiate spectrum handoff before the routing information is exchanged. When spectrum handoff occurs, the targeted node stops all ongoing communication, leaves the frequency, determines a new spectrum for transmission, identifies neighboring nodes, and informs neighboring nodes of the change in frequency. The targeted node cannot receive or transmit updated routing information until the handoff is complete; this is referred to as deafness. Until the routing information is updated, the targeted node and its neighbors will use stale routing information. By causing the targeted node to continuously perform spectrum handoff just before routing information exchange, the attack can be extended and made more severe [53].

The paper [116] presents a collision free resident channel selection based solution (CFRCS). With this solution, a resident channel is selected by each node from the available channel set during network initialization. It then broadcasts this selection with its neighbors. Nodes are expected to receive any updates on the resident channel. However, this protocol requires that each cognitive node is equipped with two half duplex transceivers with one waiting on the resident channel for a request of control message exchange, and the other sitting on the data transmission channel.

8.2. Small backoff window

The small backoff window attack is also known as the backoff manipulation attack. In this attack the attacker manipulates the contention protocol parameters to retain exclusive or more frequent access to the channel. Selfish or malicious users choose a very small backoff, or contention, window in the effort to gain more access to the channel. This attack is feasible against cognitive radio networks using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol at the MAC layer.

The authors of [98] base their proposal on the method presented in the first paper, only using a more refined test to compute the difference between distributions. A strategy is presented in which the backoff value of a sender is assigned by the corresponding receiver. Monitoring of the sender's compliance with the assigned backoff window is also provided by the receiver. If the sender deviates from the assigned value, it incurs punishment with the assignment of a larger backoff value for future transmissions. Continued misbehavior can result in the node from being ejected from the network.

The mitigation described above does not apply to events if collusion occurs between the sender and receiver. Neither does it apply if the receiver assigns large backoff values to alleviate contention for its own transmissions. Increasing the number of cognitive radios monitoring the backoff can help alleviate issues of collusion, or the event of the malicious receiver. It was suggested that every cognitive radio publish its backoff schedule in advance, or publish the seed to a publicly known pseudo random number generator used to generate the backoff values. With this information, neighbors can detect misbehavior of neighboring nodes [113].

8.3. Lion attack

The Lion attack is specific to the cognitive radio network. The attack takes place at the physical/link layer, while targeting the transport layer. In essence, the attacker uses a primary user emulation attack in order to disrupt the Transmission Control Protocol (TCP) connection. The attacker can be an outsider or a part of the network.

The attack affects the TCP by forcing frequency handoffs in vacating the channel due to the perception the primary user is present. When the handoff occurs, the TCP is not aware of the switchover. TCP will continue creating logical connections and sending packets while not receiving any acknowledgments. If no acknowledgments are returned, TCP considers the segment as lost due to congestion. As a consequence, TCP retransmits the segment while reducing the congestion window. This results in delays and packet loss, reducing throughput.

The attack can become even more extended and severe, becoming a denial of service attack, if the attacker can anticipate the new channel to which the secondary user will move. If the attacker moves to the new channel, and again simulates the primary user, or jams the channel, the sender will not be able to successfully send data [24].

The authors of the paper [43] present a method of mitigation to the lion attack. Besides identifying the attack, the authors suggest that cross-layer communication must be established in order to make the TCP aware of the attack. This communication will allow the cognitive radio network to halt the TCP connections during frequency handoff. The TCP parameters can then be adapted to the connection parameters after handoff.

Additionally, the control data that is shared by the whole group of cognitive radio network participants needs to be protected from eavesdropping by the attacker to prevent the attacker from becoming aware of the current and future actions of the network. The authors of [43] suggest the use of a common shared secret key. The group key will provide group members the ability to send encrypted data, decrypt received data, and authenticate itself as a network member. Of course, only the current group members should know the group key, so the key would need to be updated as the membership changes. It is suggested current group key management (GKM) studies be applied to the cognitive radio network as a solution. Unfortunately, the cross-layer communication and group key can only mitigate the lion attack since these solutions cannot stop denial of service or channel degradation due to jamming. In an effort to identify the attacker, the authors of [43] suggest adding a parallel cross-layer intrusion detection system adapted to cognitive radio networks.

8.4. Jellyfish attack

The jellyfish attack and the lion attack are related in that they both target the TCP. In the lion attack, the

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

degradation of the TCP occurs because of frequent frequency handoffs. In the jellyfish attack, throughput is decreased because of out of order, delayed, or dropped packets.

The jellyfish attack is performed at the network layer, while targeting the transport layer. The attacker can perpetrate the attack by intentionally reordering the packets it receives and forwards. TCP has a vulnerability to out of order packets; out of order packets trigger retransmissions and degrade network throughput. Dropping a fraction of the packets also degrades throughput, similar to a sinkhole attack. However, in this variant the packets are dropped intelligently such that they coincide with the TCP transmission window. This can cause near zero throughput in the TCP protocol. Additionally, if the malicious node randomly delays packets, throughput will be affected because it causes the TCP timers to be invalid, resulting in network congestion [53]. Part of the difficulty in mitigating the jellyfish attack is that the jellyfish obeys all of the data plane and control plane protocol rules. Therefore, supportive nodes can hardly distinguish between the attack and a congested network [64]. It is possible that successful jellyfish attacks can partition the network [75].

In the paper [75] a scheme is presented that exploits the broadcast nature of the wireless medium for detection and mitigation of jellyfish attacks. A jellyfish can be detected by its neighbors simultaneously when the neighbors are set as promiscuous so they can observe each other's activities. In the proposed scheme the TCP protocol is altered such that catalyst helper packets are sent to check for congestion when the network experiences low throughput. The packets are supplied with cumulative sequence numbers and a flow id number. Observing nodes are able to identify if packets are delayed, dropped, or sent out of order by a neighbor. When a threshold of such detected misbehavior is reached, the misbehaving node is punished, and can be isolated from the network. Punishment can include revocation of the certificate of the malicious node by the centralized trusted authority, or isolation of the malicious node by the dropping of all control and data packets forwarded or originated from the node.

A trust based mechanism is presented in [68] for establishing and managing trust in pure ad hoc networks where no base station or other central entity exists and the nodes are not required to be preconfigured. Routing protocols, such as Dynamic State Routing (DSR) and Adhoc On Demand Distance Vector (AODV), are modified to allow establishment of routes with a certain level of confidence. Nodes first check the trust value at the next hop to ensure it is equal to or greater than a specified threshold before forwarding packets to the node. If the threshold value is not adequate, the sending node will try to avoid a path using the suspect node [68].

A scalable and a robust approach to enforce collaboration in a mobile ad hoc network is presented by [36]. In this mitigation effort, every node observes its neighbors' activities. Each node computes the ratio of dropped packets in a certain time window for its neighbors that drop packets. When a ratio for a node exceeds an predetermined threshold value, the one hop neighbors punish the node with isolation for a time period.

8.5. Policy attacks

As mentioned in Section 7.2, the paper [6] describes the security threats associated with each of the main functions of the policy system of the policy based cognitive radio. The attack on the policy reasoning and enforcement functions, as well as the policy derivation and distribution functions by spoofing, were already described. The forging policy attacks occur at a different level, targeting the application layer, and are described here.

In the forgery attack against the policy derivation function the malicious entity intercepts communications from the policy administrator intended for the policy manager. The original policy is replaced with a forged policy resulting in a compromised network and decreased network performance. Similarly, the forgery attack on the policy distribution function intercepts and replaces the policy from the policy server intended for the policy engine. The use of certificates or other authentication protocols for identity validation can mitigate these attacks.

8.6. A suggested multi-level security framework as attack mitigation

Trying to address several layers of attack of the cognitive radio network, the paper [77] presents a multilevel framework for the security of the cognitive radio network. The basis of the proposal is a new, secure, adaptive MAC protocol called dynamic decentralized and hybrid MAC (DDHMAC). This cognitive radio MAC protocol is a hybrid that lies between the static common control channel using an unlicensed spectrum band (commonly referred to as GCCC) and the non-GCCC protocols. The protocol creates an adaptive, secure, and energy efficient network by tuning its parameters efficiently and intelligently based on the current situation of the network. The protocol includes a primary control channel and a backup control channel, both sent over the white spaces in the spectrum.

Four levels of security are provided by the DDHMAC protocol. First is the encryption of the beacon frame. Recipients of the beacon frame apply the relevant decryption scheme to read the primary and backup control channels.

The second level of security is the secure transmission of the free channel list (FCL). The FCL is exchanged secretly over the primary control channel. The chosen control channel is only known to the cognitive radios in the vicinity. Additionally, all frames are encrypted using the public key, and only nodes with the private key can retrieve the information.

DDHMAC adds a timestamp to each data transmission as a third level of security. Data is expected to be received in a certain period of time; if the data is not received in the specified time period, it is assumed the integrity of the data could be compromised and therefore untrustworthy. This protocol helps protect the system against man in the middle attacks.

The last level of security is the dynamicity of the control channel. Since the primary control channel is sent over a white space, the appearance of the primary user could occur, thus moving the network communication to the

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

backup control channel. If the primary user also appears on the backup control channel, the nodes switch to the GCCC to search for a beacon frame. Any attacker targeting the primary and backup control channels via smart jamming will need to recompile their attack strategy whenever the primary users appear. This provides a higher level of security to the network.

9. Conclusion

With our increasing usage of the air as a medium for connecting electronically with the world, the current spectrum defined for commercial and personal usage has become crowded. The cognitive radio network with software defined capabilities will open to users more spectrum frequencies, and hence, enhanced communication opportunities. However, the new technology also provides avenues for new attacks perpetrated by malicious or selfish users with the desire to inhibit communication, capture or change the message, or use the spectrum exclusively.

In this paper we have presented the structures of malicious attacks on the cognitive radio network. We have identified attacks from both the traditional cellular networks and the wireless sensor network arena that apply. We also presented attack scenarios specific to the cognitive radio network architecture and capabilities. Following each attack scenario we presented mitigating techniques particular to the attack.

Recent security research on the cognitive radio network has focused on the insider threat (Byzantine), jamming of the control channel or other portions of the spectrum, and externally affecting spectrum usage by masquerading as a primary user. More research needs to be completed in the area of secure transport protocols for the spectrum aware cognitive radio networks, considering the network's unique characteristics in spectrum management and spectrum mobility. Additionally, research needs to take place in the realm of cognitive radio ad hoc networks (CRAHNS), addressing their distinctive security issues related to their network building functions. Finally, further research needs to be conducted in the area of protecting the cognitive radio function from many of the traditional threats, such as worms, trojans, and viruses, as well as new threats that attack the radio's ability to learn.

As the cognitive radio network concept matures and comes to fruition, the network security sword play of thrust and parry will continue. The true challenge of the security warrior is prior preparation for the battle. Extensive research and discussion about securing the network will contribute to a proper framework that can be built into the cognitive radio system.

References

[1] What is unlicensed spectrum? What frequencies are they in? (WiMax), 2013, <http://www.wimax.com/wimaxregulatory/what-is-unlicensedspectrum-what-frequencies-are-they-in> (accessed 27.06.13).
[2] Andre Abadie, Duminda Wijesekera, Cognitive radio technologies: envisioning the realization of network centric warfare, in: Communications and Information Systems Conference (MilCIS), 2013 Military, 2012, pp. 1–7 (IEEE).
[3] Kamran Arshad, Malicious users detection in collaborative spectrum sensing using statistical tests, in: 2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN), 2012. pp. 109–113 (IEEE).
[4] Alireza Attar, Helen Tang, Athanasios V. Vasilakos, F. Richard Yu, Victor C.M. Leung, A survey of security challenges in cognitive radio networks: solutions and future research directions, Proc. IEEE 100 (12) (2012) 3172–3186.
[5] Behnam Bahrak, JungMin Park, Security of spectrum learning in cognitive radios, arXiv preprint arXiv:1304.0606, 2013.
[6] Gianmarco Baldini, Valentin Rakovic, Vladimir Atanasovski, Liljana Gavrilovska, Security aspects of policy controlled cognitive radio, in: 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), 2012, pp. 1–5.
[7] Gianmarco Baldini, Taj Sturman, Abdur Rahim Biswas, Ruediger Leschhorn, Gyozo Godor, Michael Street, Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead, Commun. Surv. Tutorial IEEE 14 (2) (2012) 355–379.
[8] Kaigui Bian, Xiaojiang Du, Xiaoming Li, Enabling fair spectrum sharing: mitigating selfish misbehaviors in spectrum contention, IEEE Network (2013) 17.
[9] Erik Blasch, Timothy Busch, Sunil Kumar, Khanh Pham, Trends in survivable/secure cognitive networks, in: 2013 International Conference on Computing, Networking and Communications (ICNC), 2013, pp. 825–829 (IEEE).
[10] Marcelo Camilo, David Moura, Juraci Galdino, Ronaldo M. Salles, Antijamming defense mechanism in cognitive radios networks, in: Military Communications Conference, 2012-MILCOM 2012, 2012, pp. 1–6 (IEEE).
[11] Aldo Cassola, Tao Jin, Guevara Noubir, Bishal Thapa, Efficient spread spectrum communication without pre-shared secrets, Mobile Comput. IEEE Trans. 12 (8) (2013) 1669–1680.
[12] Agnes Chan, Xin Liu, Guevara Noubir, Bishal Thapa, Broadcast control channel jamming: resilience and identification of traitors, in: IEEE International Symposium on Information Theory, 2007. ISIT 2007, 2007, pp. 2496–2500 (IEEE).
[13] Changlong Chen, Min Song, Chunsheng Xin, Mansoor Alam, A robust malicious user detection scheme in cooperative spectrum sensing, in: Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 4856–4861.
[14] Changlong Chen, Min Song, ChunSheng Xin, Jonathan Backens, A game theoretical anti-jamming scheme for cognitive radio networks, IEEE Network (2013).
[15] Chao Chen, Hongbing Cheng, Yu Dong Yao, Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack, Wirel. Commun. IEEE Trans. 10 (7) (2011) 2135–2141.
[16] Ruiliang Chen, JungMin Park, Jefrey H. Reed, Defense against primary user emulation attacks in cognitive radio networks, Sel. Areas Commun. IEEE J. 26 (1) (2008) 25–37.
[17] WenLong Chin, ChunLin Tseng, ChunShen Tsai, WeiChe Kao, ChunWei Kao, Channel based detection of primary user emulation attacks in cognitive radios, in: Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, 2012, pp. 1–5 (IEEE).
[18] T. Charles Clancy, Nathan Goergen, Security in cognitive radio networks: threats and mitigation, in: 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. Crown Com 2008, 2008, pp 1–8 (IEEE).
[19] Roberto Di Pietro, Gabriele Oligeri, Jamming mitigation in cognitive radio networks, IEEE Network (2013).
[20] John R. Douceur, The Sybil attack, in: Peer-to-Peer Systems, Springer, 2002, pp. 251–260.
[21] De Du, Soft reputation based secure cooperative spectrum sensing, in: 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1, 2012, pp. 463–467 (IEEE).
[22] Lingjie Duan, Alexander W. Min, Jianwei Huang, Kang G. Shin, Attack prevention for collaborative spectrum sensing in cognitive radio networks, Sel. Areas Commun. IEEE J. 30 (9) (2012) 1658–1665.
[23] Rajni Dubey, Sanjeev Sharma, Lokesh Chouhan, Secure and trusted algorithm for cognitive radio network, in: 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), 2012, pp. 1–7 (IEEE).
[24] Wassim ElHajj, Haidar Safa, Mohsen Guizani, Survey of security issues in cognitive radio networks, J. Internet Technol. 12 (2) (2011) 181–198.
[25] Mohammed Farrag, Mostafa ElKhamy, Mohamed ElSharkawy, C44. Secure cooperative blindly optimized compressive spectrum sensing for cognitive radio, in: 2012 29th National Radio Science Conference (NRSC), 2012, pp. 533–540 (IEEE).

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

[26] Koorosh Firouzbakht, Guevara Noubir, Masoud Salehi, On the capacity of rate adaptive packetized wireless communication links under jamming, in: Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, 2012, pp. 3–14 (ACM).

[27] A. Fragkiadakis, E. Tragos, I. Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks, Commun. Surveys Tutorials IEEE 15 (1) (2013) 428–445.

[28] Maryam Haghighat, Seyed Mohammad, Sajad Sadough, Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks, in: 2012 Sixth International Symposium on Telecommunications (IST), 2012, pp. 148–151 (IEEE).

[29] Dong Hao, Kouichi Sakurai, A differential game approach to mitigating primary user emulation attacks in cognitive radio networks, in: 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), 2012, pp. 495–502 (IEEE).

[30] Paul K. Harmer, Michael A. Temple, An improved LFS engine for physical layer security augmentation in cognitive networks, in: 2013 International Conference on Computing, Networking and Communications (ICNC), 2013, pp. 719–723 (IEEE).

[31] Xiaofan He, Huaiyu Dai, Peng Ning, A Byzantine attack defender in cognitive radio networks: the conditional frequency check, Wirel. Commun. IEEE Trans. 12 (5) (2013) 2512–2523.

[32] L. Hou, K.H. Yeung, K.Y. Wong, A virus spreading model for cognitive radio networks, Physica A (2012).

[33] Hu Nansai, Yu Dong Yao, Joseph Mitola, Most active band (mab) attack and countermeasures in a cognitive radio network, Wirel. Commun. IEEE Trans. 11 (3) (2012) 898–902.

[34] Y.C. Hu, Adrian Perrig, David B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies, vol. 3, 2003, pp. 1976-1986 (IEEE).

[35] Shraboni Jana, Kai Zeng, Prasant Mohapatra, Trusted collaborative spectrum sensing for mobile cognitive radio networks, in: INFOCOM, 2012 Proceedings IEEE, 2012, pp. 2621–2625 (IEEE).

[36] Ning Jiang, Kien A. Hua, Danzhou Liu, A scalable and robust approach to collaboration enforcement in mobile ad hoc networks, J. Commun. Netw. 9 (1) (2007) 56.

[37] Z. Jin, S. Anand, K. Subbalakshmi, Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks, 2012.

[38] Minho Jo, Longzhe Han, Dohoon Kim, Hoh Peter In, Selfish attacks and detection in cognitive radio ad hoc networks, IEEE Netw. 27 (3) (2013).

[39] Sanket S. Kalamkar, Adrish Banerjee, Ananya Roychowdhury, Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using Dixon's outlier detection method, in: 2012 National Conference on Communications (NCC), 2012, pp. 1–5 (IEEE).

[40] Chris Karlof, David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Netw. 1 (2) (2003) 293–315.

[41] Anubhuti Khare, Manish Saxena, Roshan Singh Thakur, Khyati Chourasia, Attacks & preventions of cognitive radio networks survey, Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) 2 (3) (2013) 1002.

[42] Loukas Lazos, Sisi Liu, Marwan Krunz, Mitigating control channel jamming attacks in multichannel ad hoc networks, in: Proceedings of the Second ACM Conference on Wireless Network Security, 2009, pp. 169–180 (ACM).

[43] Olga Leon, Juan Hernandez-Serrano, Miguel Soriano, A new cross-layer attack to TCP in cognitive radio networks, in: Second International Workshop on Cross-layer Design, 2009. IWCLD'a9, 2009, pp. 1–5 (IEEE).

[44] Olga. Leon, Juan. Hernandez-Serrano, Miguel. Soriano, Securing cognitive radio networks, Int. J. Commun Syst 23 (5) (2010) 633–652.

[45] Feng Lin, Zhen Hu, Shujie Hou, Jingzhi Yu, Changchun Zhang, Nan Guo, Michael Wicks, Robert C. Qiu, Kenneth Currie, Cognitive radio network as wireless sensor network (ii): security consideration, in: Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON), 2011, pp. 324–328 (IEEE).

[46] Sheng Liu, Haojin Zhu, Shuai Li, Xu Li, Cailian Chen, Xinping Guan, An adaptive deviation tolerant secure scheme for distributed cooperative spectrum sensing, in: 2012 IEEE Global Communications Conference (GLOBECOM), 2012, pp. 603–608.

[47] Sisi Liu, Loukas Lazos, Marwan Krunz, Thwarting inside jamming attacks on wireless broadcast communications, in: Proceedings of the Fourth ACM Conference on Wireless Network Security, 2011, pp. 29–40 (ACM).

[48] Sisi Liu, Loukas Lazos, Marwan Krunz, Thwarting control channel jamming attacks from inside jammers, Mobile Comput. IEEE Trans. 11 (9) (2012) 1545–1558.

[49] Brandon F. Lo, A survey of common control channel design in cognitive radio networks, Phys. Commun. 4 (1) (2011) 26–39.

[50] Brandon F. Lo, Ian F. Akyildiz, Multiagent jamming resilient control channel game for cognitive radio ad hoc networks, in: 2012 IEEE International Conference on Communications (ICC), 2012, pp. 1821–1826 (IEEE).

[51] KaiWang Lu, HaiZhou Ke, Jie Yang, LiangJun Zhang, Research of PUE attack based on location, in: 2012 IEEE 11th International Conference on Signal Processing (ICSP), vol. 2, 2012, pp. 1345–1348 (IEEE).

[52] Liangping Ma, ChienChung Shen, Bo Ryu, Single radio adaptive channel algorithm for spectrum agile wireless ad hoc networks, in: 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007, 2007, pp. 547–558 (IEEE).

[53] Chetan N. Mathur, K.P. Subbalakshmi, Security issues in cognitive radio networks, Cogn. Netw. Towards Self-Aware Netw. (2007).

[54] Natarajan Meghanathan, A comprehensive review and analysis of solutions for different layers of the TCP/IP layer stack and security issues for cognitive radio networks, Int. J. Adv. Technol. 4 (1) (2013) 1–27.

[55] Natarajan Meghanathan, A survey on the communication protocols and security in cognitive radio networks, Int. J. Commun. Netw. Inform. Secur. (IJCNIS) 5 (1) (2013).

[56] Albena Mihovska, Ramjee Prasad, Elias Z. Tragos, Vangelis Angelakis, Design considerations for a cognitive radio trust and security framework, in: 2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2012, pp. 156–158 (IEEE).

[57] Joseph Mitola III, Gerald Q. Maguire Jr., Cognitive radio: making software radios more personal, Person. Commun. IEEE 6 (4) (1999) 13–18.

[58] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, The Sybil attack in sensor networks: analysis & defenses, in: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, 2004, pp. 259–268 (ACM).

[59] Seyed Morteza Mirhoseni Nezhadal, Reza Berangi, Mahmood Fathy, Common control channel saturation detection and enhancement in cognitive radio networks, Int. J. 3 (2012).

[60] Gosan Noh, Sungmook Lim, Seokwon Lee, Daesik Hong, Goodness of fit based malicious user detection in cooperative spectrum sensing, in: 2012 IEEE Vehicular Technology Conference (VTC Fall), 2012, pp. 1–5 (IEEE).

[61] Guevara Noubir, Rajmohan Rajaraman, Bo Sheng, Bishal Thapa, On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming, in: Proceedings of the Fourth ACM Conference on Wireless Network Security, 2011, pp. 97–108 (ACM).

[62] Sazia Parvin, Farookh Khadeer Hussain, Trust based security for community based cognitive radio networks, in: 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), 2012, pp. 518–525 (IEEE).

[63] Sazia Parvin, Farookh Khadeer Hussain, Omar Khadeer Hussain, Song Han, Biming Tian, Elizabeth Chang, Cognitive radio network security: a survey, J. Netw. Comput. Appl. (2012).

[64] Ms. Hetal, P. Patel, Minubhai B. Chaudhari, Survey: impact of jellyfish on wireless ad hoc network, Int. J. Eng. 1 (9) (2012).

[65] Qingqi Pei, Lei Li, Hongning Li, Beibei Yuan, Adaptive trust management mechanism for cognitive radio networks, in: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 826–831 (IEEE).

[66] Qingqi Pei, Beibei Yuan, Lei Li, Hongning Li, A sensing and etiquette reputation based trust management for centralized cognitive radio networks, Neurocomputing (2012).

[67] Federico Penna, Yifan Sun, Lara Dolecek, Danijela Cabric, Detecting and counteracting statistical attacks in cooperative spectrum sensing, Signal Process. IEEE Trans. 60 (4) (2012) 1806–1822.

[68] Asad A. Pirzada, Chris McDonald, Trust establishment in pure ad hoc networks, Wireless Pers. Commun. 37 (12) (2006) 139–168.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

[69] A. Popescu, Cognitive radio networks, Communications (COMM), 2012 9th International Conference, 2012, pp. 11–15.
[70] Sarah Purewal, Wireless Devices Outnumber Us Population, Survey Says (pcworld), 2011, <http://www.pcworld.com/article/241826/> (accessed 27.05.13).
[71] Lijun Qian, Xiangfang Li, Shuangqing Wei, Cross-layer detection of stealthy jammers in multi-hop cognitive radio networks, in: 2013 International Conference, Computing, Networking and Communications (ICNC), 2013, pp. 1026–1030.
[72] H.M. Qusay, D. MAHMOU, Cognitive Networks: Towards Self-Aware Networks, Wiley, London, 2007.
[73] Ankit Singh Rawat, Priyank Anand, Hao Chen, Pramod K. Varshney, Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks, Signal Process. IEEE Trans. 59 (2) (2011) 774–786.
[74] Kui Ren, Qian Wang, Opportunistic spectrum access: from stochastic channels to non-stochastic channels, Wirel. Commun. IEEE 20 (3) (2013).
[75] Fahad Samad, Securing Wireless Mesh Networks: A Three Dimensional Perspective. PhD thesis, Universitts bibliothek, 2011.
[76] Jaydip Sen, Security and Privacy Challenges in Cognitive Wireless Sensor Networks. arXiv preprint arXiv:13a2.2253, 2013.
[77] Munam Ali Shah, Sijing Zhang, Carsten Maple, A novel multifold security framework for cognitive radio wireless ad hoc networks, in: 2012 18th International Conference on Automation and Computing (ICAC), 2012, pp. 1–6 (IEEE).
[78] Zhihui Shu, Yi Qian, Song Ci, On physical layer security for cognitive radio networks, IEEE Network 27 (3) (2013).
[79] Sangeeta Singh, Aditya Trivedi, Anti-jamming in cognitive radio networks using reinforcement learning algorithms, in: 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), 2012, pp. 1–5 (IEEE).
[80] Shabnam Sodagari, T. Charles Clancy, An anti-jamming strategy for channel access in cognitive radio networks, in: Decision and Game Theory for Security, Springer, 2011, pp. 34–43.
[81] Yi Song, Jiang Xie, Finding out the liars: fighting against false channel information exchange attacks in cognitive radio ad hoc networks, in: 2012 IEEE Global Communications Conference (GLOBECOM), 2012, pp. 2095–2100.
[82] CaLynna Sorrells, Lijun Qian, Husheng Li, Quickest detection of denial of service attacks in cognitive wireless networks, in: 2012 IEEE Conference on Technologies for Homeland Security (HST), 2012, pp. 580–584 (IEEE).
[83] Mario Strasser, S. Capkun, M. Cagalj, Jamming resistant key establishment using uncoordinated frequency hopping, in: IEEE Symposium on Security and Privacy, 2008. SP 2008, 2008, pp. 64–78 (IEEE).
[84] A.C. Sumathi, R. Vidhyapriya, Security in cognitive radio networks survey, in: 2012 12th International Conference on Intelligent Systems Design and Applications (ISDA), 2012, pp. 114–118 (IEEE).
[85] Richard S. Sutton, Andrew G. Barto, Reinforcement Learning: An Introduction, Cambridge Univ Press, 1998. vol. 1.
[86] Patrick Tague, Mingyan Li, Radha Poovendran, Probabilistic mitigation of control channel jamming via random key distribution, in: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007, 2007, pp. 1–5 (IEEE).
[87] Patrick Tague, Mingyan Li, Radha Poovendran, Mitigation of control channel jamming under node capture attacks, IEEE Trans. Mob. Comput. 8 (9) (2009).
[88] Kefeng Tan, Shraboni Jana, Parth H. Pathak, Prasant Mohapatra, On insider misbehavior detection in cognitive radio networks, IEEE Netw. (2013) 5.
[89] Yi Tan, Kai Hong, Shamik Sengupta, K.P. Subbalakshmi, Using Sybil identities for primary user emulation and byzantine attacks in DSA networks, in: 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011), 2011, pp. 1–5 (IEEE).
[90] Yi Tan, Shamik Sengupta, K.P. Subbalakshmi, Primary user emulation attack in dynamic spectrum access networks: a game theoretic approach, Commun. IET 6 (8) (2012) 964–973.
[91] Long Tang, Wu Juebo, Research and analysis on cognitive radio network security, Wirel. Sens. Netw. 4 (4) (2012) 120–126.
[92] Deepraj S. Vernekar, An Investigation of Security Challenges in Cognitive Radio Networks, 2012, <http://digitalcommons.unl.edu/ceendiss/20/>.
[93] Beibei Wang, Yongle Wu, KJ Ray Liu, T Charles Clancy, An anti-jamming stochastic game for cognitive radio networks, Sel. Areas Commun. IEEE J. 29 (4) (2011) 877–889.
[94] Qian Wang, Kui Ren, Peng Ning, Anti-jamming communication in cognitive radio networks with unknown channel statistics, in: 2011 19th IEEE International Conference on Network Protocols (ICNP), 2011, pp. 393–402 (IEEE).
[95] Qian Wang, Xu Ping, Kui Ren, XiangYang Li, Towards optimal adaptive UFH based anti-jamming wireless communication, Sel. Areas Commun. IEEE J. 30 (1) (2012) 16–30.
[96] Wenjing Wang, Shameek Bhattacharjee, Mainak Chatterjee, Kevin Kwiat, Collaborative jamming and collaborative defense in cognitive radio networks, Pervasive Mobile Comput. (2012).
[97] Wenkai Wang, Husheng Li, Yan Sun, Zhu Han, Attack proof collaborative spectrum sensing in cognitive radio networks, in: 43rd Annual Conference on Information Sciences and Systems, 2009. CISS 2009, 2009, pp. 130–134 (IEEE).
[98] Wenkai Wang, Yan Sun, Husheng Li, Zhu Han, Cross-layer attack and defense in cognitive radio networks, in: 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), 2010, pp. 1–6 (IEEE).
[99] Hong Wen, Shaoqian Li, Xiping Zhu, Liang Zhou, A framework of the PHY layer approach to defense against security threats in cognitive radio networks, IEEE Netw. (2013).
[100] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A survey of attacks and countermeasures in mobile ad hoc networks, in: Wireless Network Security, Springer, 2007, pp. 103–135.
[101] Yongle Wu, Beibei Wang, KJRay Liu, TCharles Clancy, Anti-jamming games in multichannel cognitive radio networks, Selected Areas Commun. IEEE J. 30 (1) (2012) 4–15.
[102] Alexander M. Wyglinski, Maziar Nekovee, Thomas Hou, Cognitive Radio Communications and Networks: Principles and Practice, Academic Press, 2009.
[103] Hua Xiao, Kai Yang, Xiaodong Wang, Huaizong Shao, A robust MDP approach to secure power control in cognitive radio networks, in: 2012 IEEE International Conference on Communications (ICC), 2012, pp. 4642–4647 (IEEE).
[104] Liang Xiao, W. Sabrina Lin, Yan Chen, K.J. Liu, Indirect reciprocity game modeling for secure wireless networks, in: 2012 IEEE International Conference on Communications (ICC), 2012, pp. 928–933 (IEEE).
[105] Sumit Yadav, Manisha J. Nene. RSS based detection and expulsion of malicious users from cooperative sensing in cognitive radios, in: 2013 IEEE 3rd International Advance Computing Conference (IACC), 2013, pp. 181–184 (IEEE).
[106] Qiben Yan, Ming Li, Tingting Jiang, Wenjing Lou, Y. Thomas Hou, Vulnerability and protection for distributed consensus based spectrum sensing in cognitive radio networks, in: 2012 Proceedings IEEE INFOCOM, 2012, pp. 900–908 (IEEE).
[107] Seung Yi, Prasad Naldurg, Robin Kravets, Security aware ad hoc routing for wireless networks, in: Proceedings of the 2nd ACM International Symposium on Mobile ad hoc Networking for Computing, 2001, pp. 299–302 (ACM).
[108] Zhou Yuan, Dusit Niyato, Husheng Li, Ju Bin Song, Zhu Han, Defeating primary user emulation attacks using belief propagation in cognitive radio networks, Sel. Areas Commun. IEEE J. 30 (10) (2012) 1850–1860.
[109] Saman T. Zargar, Martin B.H, Weiss, Carlos E. Caicedo, James B.D. Joshi, Security in Dynamic Spectrum Access Systems: A Survey, University of Pittsburgh, 2011, <http://d-scholarship.pitt.edu/2823/>.
[110] Chaorui Zhang, Rong Yu, Yan Zhang, Performance analysis of primary user emulation attack in cognitive radio networks, in: 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), 2012, pp. 371–376 (IEEE).
[111] Haopeng Zhang, Zhenyi Liu, Qing Hui, Optimal defense synthesis for jamming attacks in cognitive radio networks via swarm optimization, in: 2012 IEEE Symposium on Computational Intelligence for Security and Defence Applications (CISDA), 2012, pp. 1–8 (IEEE).
[112] Lu Zhang, Qingqi Pei, Hongning Li, Anti-jamming scheme based on zero pre-shared secret in cognitive radio network, in: 2012 Eighth International Conference on Computational Intelligence and Security (CIS), 2012, pp. 670–673 (IEEE).
[113] Yan Zhang, Loukas Lazos, Vulnerabilities of cognitive radio mac protocols and countermeasures, IEEE Netw. (2013) 41.
[114] Caidan Zhao, Wumei Wang, Lianfen Huang, Yan Yao, Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio, in: 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009. WiCom'a9, 2009, pp. 1–5 (IEEE).

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001

[115] Jing Zhao, Guohong Cao, Robust topology control in multi-hop cognitive radio networks, in: 2012 Proceedings IEEE INFOCOM, 2012, pp. 2032–2040 (IEEE).
[116] Xiangquan Zheng, Ying Li, Haicheng Zhang, A collision free resident channel selection based solution for deafness problem in the cognitive radio networks, in: 2010 IEEE International Conference on Wireless Information Technology and Systems (ICWITS), pp. 1–4 (IEEE), 2010.

Deanna T. Hlavacek is pursuing her Ph.D. in Information Assurance in the Department of Electrical and Computer Engineering at Iowa State University in Ames, Iowa. She was trained as a meteorologist and served in the United States Air Force. She retired from the USAF in 2010 with the rank of Lieutenant Colonel. Deanna obtained her Master's Degree in Computer Science at Northern Illinois University in 2005, and worked as a Software Engineer for Tellabs in Naperville, Illinois. She is a student member of IEEE, and a member of the electrical and computer engineering honor society, Eta Kappa Nu.

J. Morris Chang is an associate professor at Iowa State University. Dr. Chang received his Ph.D. in computer engineering from North Carolina State University. His industry experience includes positions at Texas Instruments, Microelectric Center of North Carolina and AT&T Bell Laboratories. He received the University Excellence in Teaching Award at Illinois Institute of Technology in 1999. Dr. Chang's research interests include: Cyber Security, Wireless Networks, and embedded computer system. Currently, he is a handling editor of Journal of Microprocessors and Microsystems and the Associate Editor-in-Chief of IEEE IT Professional. He is a senior member of IEEE.

Please cite this article in press as: D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.001