COUNTER MEASURES FOR LINK LAYER ATTACKS IN COGNITIVE RADIO NETWORKS: 
A DETAILED STUDY

Shruthi N1, Vinay C K2
1Department of ECE, Assistant Professor, APS College of Engineering, Bangalore
2Hewlett Packard Application Services, Bangalore

Abstract: An ever-existing concern is the lack of security due to the very fact that the technology is wireless and is vulnerable to security threats & attacks. Also, among the wide-spread characteristics of a CR, self-organized security management is one of prime considerations. Each layer in cognitive radios is susceptible to widespread threats and security attacks. In fact, the scope of this paper reveals a detailed tabulation of the possible security threats/attacks faced by cognitive radios & cognitive radio networks in the Link and MAC layer, along with the current state-of-the-art to detect the corresponding attacks and discuss the possible countermeasures for the same. The possible security approaches for attacks in different layers can be generalized as use of spread spectrum techniques and error correcting codes, use of MAC layer admission control mechanism, authentication and cryptography algorithms. However, the paper makes an attempt to effectively survey the existing detection techniques as well as countermeasures relevant to the Link layer and MAC layer.

Keywords—Cognitive Radio, Link layer, MAC layer, network security, countermeasures, protocols.

I. EVOLUTION OF COGNITIVE RADIO (CR)
The major problem arising in the wireless domain is spectrum scarcity. Even the spectrum allocation policies contribute to the scarcity problem since they do not exploit the fact that RF spectrum is time and location varying. In spite of having provided the users with an unlicensed band (ISM – Industrial, Medical & Scientific), the scarcity problem could not be solved completely. The FCC (Federal Communications Commission) had earlier in 1985 declared selected portions of the spectrum as license-free. As quoted in several studies, there exist many under-utilized static parts in the allocated spectrum. FCC’s reference [1] states that the assigned spectrum utilization is around 15% to 85%, subject to geographical and temporal variations.

Due to overcrowded users, there is a substantial increase in interference and contention between networking devices. A possible solution to this was to allow unlicensed users to access the licensed band (below 900 MHz & in the 3 GHz band) without interfering with the operation of the privileged licensed users. Sometimes, these statically allocated spectrums may be underutilized. The Wireless Research Center (WRC) has shown experimental results that majority of the 1 GHz to 10 GHz spectrum is underutilized [2]. A possibly effective solution proposed to utilize the spectrum was the CR. It is the revolutionary evolution of software radio. CRs are intelligent novel devices which utilize the free portions (“white spaces” or “spectrum holes”) by sensing the spectrum. Spectrum hole is defined as a band of frequencies which has been allotted to some primary user (PU), but is not being used by that PU at that instant of time at a particular geographical location. CR is a radio that is capable of adapting to changes in the environment (in the form of signals and channels) which gets its communication parameters altered so that the secondary users (SUs) in the spectrum can benefit from efficient spectrum utilization [3]. PUs, also called “incumbent” users hold a valid license to access a fixed portion of the spectrum. Secondary Users, also termed as “cognitive” users opportunistically use the available spectrum portions without affecting the usage of the PUs.

II. SECURITY OBJECTIVES OF CR NETWORKS
Cognitive radio networks (CRNs) evolved with the conceptualization of the idea that rather than having intelligence reside in a single device as a CR, intelligence can reside in a network itself. They are self-organizing, intelligent networks which adapt to the environmental changes in real-time. These networks along with Dynamic Spectrum Access (DSA) capabilities diligently help enhance the spectrum efficiency as well as the network capacity. CRNs are quite complex systems and a lot of effort goes into netting its components together for existent working under realistic conditions. CRNs can be categorized based on their architectures as:
(i) Infrastructure architecture: An infrastructure CRN has access points/base stations.
(ii) Ad-Hoc: Ad-Hoc networks use devices to establish communication links between nodes based on existing communication protocols (e.g. Bluetooth, Wi-Fi). Ad-Hoc networks do not require base stations as Infrastructure CRNs do.
(iii) **Mesh:** These CRNs combine the concepts of both the above CRNs. The devices in these kinds of networks connect to base stations through neighbouring devices. The common security objectives of a generic CR Network are:

(i) **CONFIDENTIALITY:** No access of network data to unauthorized users. Confidentiality is accomplished by implementing ciphers and data encryption wherein the access key is provided only to the authenticated user. Data decryption and accessibility is achieved only by users possessing this secret key.

(ii) **INTEGRITY:** Avoid changes to transmit data. Mostly, in wireless networks data transmitted is more prone to intruders and obstacles. There definitely arises a need for an extra security layer to ensure reliability and security in wireless communication and integrity aims at achieving this.

(iii) **AVAILABILITY:** Refers to availability of network resources to meet user demands of resources in dynamic and unpredictable operating conditions. Resources may include nodal information, source data, and transmission medium and so on. Availability refers to the availability of secondary base stations in centralized CRNs. The ad hoc network cannot make any assumptions regarding the availability of nodes at a given time instant since few of the nodes may even be dormant/idle or shut down once in a while. Also, attacks and topology changes hindering the robustness of the routing fabric need to be controlled by the routing protocols to balance network connectivity [4].

(iv) **ACCESS CONTROL:** Access control is a security requirement for the physical layer. Users must be guaranteed to have access to the network, and they must obey their organization’s policy. At the application level, restrict the available network resources/services only to authorized users. The network layer routing protocol must ensure that no unauthorized used join a packet forwarding group. Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based access control (RBAC) are few of the approaches to access control. DAC allows the restriction of access to objects based on the identity of subjects or groups of subjects while MAC involves centralized mechanisms to control the access to objects with formal authorization policy. RBAC applies the concept of roles within the subjects and objects.

(v) **AUTHENTICITY/NON-REPUDIATION:** Routing traffic leaves behind traces to ensure that all parties responsible for data propagation do not later deny participation in the routing network. All authenticated users of a network trust a centralized certificate authority (CA). The peer participants request the CA for identity signatures. Digitally signed certificates are exchanged and verified by peers to ensure security and approve initiation of data transmission. However, this method of authentication may sometimes be quite challenging in distributed CRNs due to randomly distributed SUs affecting the licensed PU’s transmission activity.

III. CLASSIFICATION OF ATTACKS BASED ON THE LAYERS ATTACKED

There are a variety of ways in which network attacks can be classified. However, the point of focus in this technical survey paper is the classification based on the layers. The attacks on CRNs can be categorized into mainly four classes. They are:

- **Physical Layer attacks,**
- **Link Layer (MAC Layer) attacks,**
- **Network Layer attacks,**
- **Transport Layer attacks.**

In general, the attacks target the Physical, Network & MAC layers. Due to the Dynamic Spectrum Access (DSA) strategy in CR, the PHY layer in CR is more complex than a conventional wireless communication system and is more likely to be attacked. The predominant types of PHY layer attacks include the Primary User Emulation Attack (PUEA), Reporting False Sensing Data (RFSD), Objective Function Attack and Jamming. Some predominant types of Link Layer attacks are [2] Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DoS attack (CCSD) and Selfish Channel Negotiation (SCN). Since, MAC layer is a sub layer of the Data Link layer, threats/attacks in the MAC layer are often termed as Link layer attacks in a broader picture. Some of the major MAC layer attacks can be Common Control Channel (CCC) attacks including MAC spoofing, Congestion attacks and Jamming attacks, Beacon Falsification (BF) attacks and so on. Some of the major types of Network layer attacks include Redirection attack where packets are redirected in the wrong direction forcing poor network, Sybil attack wherein a node illegitimately claims multiple identities and is a harmful attack against sensor and ad hoc networks and Routing attacks like HELLO Flood attack and Sinkholes. The major types of Transport layer attack include the LION attack, flooding and De-Synchronization. Since CRs adopt layered architecture, cross-layers attacks and Software defined radio (SDR) attacks which are common to multiple layers are possible to occur. One such instance is a combination of a SSDF attack with a small-back off-window attack (SBW) & the lion attack. Similarly, Denial of Service (DoS) attacks and jamming can be launched in both PHY and MAC layers.

IV. THE LINK LAYER ATTACKS

Link layer has the responsibility of transferring data from one node to the next node in one hop, which provides the functional means to allow fragmentation of data, error correction and modulation [5]. This is
the second layer in the network protocol stack. The Data Link Layer is responsible for medium access, error control, multiplexing of data streams and data frame detection. It ensures reliable point to point and point to multi hop connections in the network. DLL detect and correct the transmission errors using error correction method. This layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel. Data link layer protocols include, SMACS (Self-Organized Medium Access Control for Sensor Networks), EARS (Eavesdrop and Register). Most of the link layer attacks detect a malicious entity masquerading as a primary user. Irrespective of whether it is the case of centralized or decentralized networks, malicious transmitters must be distinguished from authenticated primaries and this must be facilitated by digital cryptography techniques. The medium access control (MAC) layer is one of the important sub layers of the link layer, which controls channel assignment. MAC layer attacks introduce large delays and increase energy drain in individual nodes. It hence becomes mandatory for any network engineer to counter both Link layer and MAC layer attacks. An attempt to briefly describe the major Link and MAC layer attacks and solutions follows.

A. Beacon Falsification (BF) Attacks
The main characteristic of the BF attack is the disruption of synchronization between IEEE 802.22 WRANs (Wireless Regional Access Networks). The inter-cell beacons are forged with arbitrarily large CCN values. The throughput of multiple, overlapping WRANs might decrease if all intend to use the same spectrum band simultaneously. Interference caused to incumbent receivers may be another concern. To facilitate a solution to this problem, self-coexistence (SC) has been proposed which consists of two types:

- **Inter-cell synchronization**
- **Inter-BS dynamic resource sharing.**

The control messages used in self-coexistence are in the form of cell beacons. Base station (BS) beacons provide information about traffic schedule and current operating parameters which are shared between BS’s of neighbouring cells [6]; while Consumer Premise Equipment (CPE) beacons inform the associated with information about the traffic flow between the BS and the CPE. An adversary can cause a BF attack by transmitting spurious beacons that contain a very large Channel Contention Number (CCN). Beacons have a signature obtained from public key cryptography. The signature is added in the beacon frame. The destinations BSs use the public key of the beacon-transmitting BS to verify the signature. On successful verification, the On-Demand Spectrum Contention (ODSC) protocol is initiated else the beacon is discarded. BF attacks are addressed by an optional authentication mechanism.

Some of the solutions proposed to counter the BF attacks by thwarting the forgery of inter-cell beacons are an inter-cell key management scheme implemented using a backhaul infrastructure to connect multiple cells and a distributed key management scheme.

B. Smaller Back-Off Window (SBW) Attacks
This attack employs the IEEE 802.11 DCF (Distributed Coordination Function) as the channel coordination mechanism [7]. Typically, a node backs off for a random time within a maximum duration window to gain channel access. This is based on the number of times the node has backed off so far and the maximum back-off duration when a node backs off for the first time. For fair channel access to all competent nodes, the back-off time should typically increase. But, a malicious node eyeing for retransmissions may operate with a smaller back-off window. A cumulative distribution function (CDF)-based solution has been proposed by authors in [8] which was improved by authors of [9]. The idea is to have a node observe the transmission attempts of its neighbour node and compare the observed CDF of the back-off time window with that of a theoretical hypothetical CDF, expected of a non-malicious node in a certain neighbourhood. The node is marked as malicious if a series of such mismatches result; an alarm is raised to indicate this intrusion.

C. MAC Spoofing
Attackers use an “evil twin” or “man-in-the-middle” attack to disrupt the CRN operation by sending unintended messages. An intruder can break into a very secure network by alternating a MAC address on a network interface. Multi-hop CRNs are more prone to such attacks since there is no central station to control/manage authenticated, integrated communication between nodes. In an enterprise deployment, for mutual understanding between a client and the infrastructure, Spoofing attacks can be mitigated using extensible authentication protocol (EAP) methods that allow mutual authentication.

D. Jamming Attacks
Genuine PUs and SUs are denied service due to these jamming attacks in a CRN in both PHY as well as MAC layers. The author in [7] states a reference with respect to the 4 types of jamming attacks: Constant jammer, Deceptive jammer, Random jammer, and Reactive jammer. Another prominently rising type is Distributed Jamming Attack which can cause a phase transition in the performance of the target network [10]. Percolation theory explains the phase transition; however, significant solutions for such attacks are yet to brighten up. A constant continuously sends packets of data irrespective of the presence of other users sharing the same channel. A deceptive jammer forces
a genuine user to move to “receive” state as they detect a constant stream of incoming data packets. A random jammer takes random breaks while sending jamming signals. A reactive jammer is an all-time active channel sensor which transmits the jamming signals upon detection. Some jamming detection techniques are discussed below:

- The authors in [11] propose a jamming detection technique that leverages the relationship between signal strength (SS) and packet delivery ratio (PDR). If a node’s relative value of SS is high and PDR is low with respect to its neighbours, it is said to be jamming-attacked.

- The Location Consistency Checks technique, suggested in [11] itself identifies a jammed node if its neighboring nodes possess lower PDR values.

- Stochastic swarm intelligence-based optimization algorithms [12] and Markov decision process based models [13] can have detect jamming attacks from multiple sources simultaneously by studying the access patterns of attackers.

Some solutions proposed to handle jamming attacks are as below:

- The link-layer defense [14] – frequency hopping (switch to a different channel) or channel surfing. Once a jamming attack is detected, communicators jump to a different channel.

- The network layer defense – spatial retreat - legitimate users change their location to escape from the interference range imposed by an attacker.

- For single channel CRNs, the Maximum Likelihood Estimation trained decision engine derives the channel hopping sequence so that SUs are prevented from jamming attacks. Q learning [15] helps the decision engine with required information.

- For multi-channel CRNs, transmission power used for the SUs on these channels is varied randomly and the probability distribution of the allocated power on the channels is generated from a Colonel Blotto game [16]-based decision engine.

- To negate a jamming attack perpetrated through channel hopping [17], switching between data and control channels is a good option, thereby enhancing throughput and efficiency. Interaction between secondary users and attackers is modeled as a zero-sum stochastic game with two players [18].

Secondary users are considered as a single player, and the second player is an attacker trying to jam as many data and/or control channels as possible. At each state of the game, secondary users analyze different parameters such as channel availability and quality and the attacker's strategy. Based on this information and applying the min-max Q learning algorithm, an optimum network configuration can be derived pertaining to channel selection and its assignment to data or control messages.

- [19] Proposes machine learning/game theory-based approaches to defend jamming attacks considering the fact that the Markov decision process-based hopping is a good approximation to the game equilibrium. SUs have extended access to multiple channels and a jamming game formulated with the transmission cost considered has been facilitated.

- A Jamming Evasive Network-coding Neighbour-discovery algorithm for a CRN in a distributed and asynchronous method has been proposed by authors of [20].

- Dynamic CCC allocation and CCC Key distribution are two anti-jamming solutions for cooperative CRNs. The former can be accomplished using cross-channel communication [21] and frequency hopping [22]. The paper [23] proposes a proactive frequency hopping protocol with pseudo-random channel switching where the optimal frequency hopping parameters are computed. A rapid frequency hopping scheme presented in [24] avoids narrow-band jamming. The concept is to intimate the CR users about a new CCC for receiving control messages in case of a currently jammed CCC. However, the latter is more robust for jamming attacks in spite of its increased overhead. The idea is to use multiple CCC channels for transmitting control signals. The random key distribution approach [25, 26] has been observed to be the most effective approach for CCC key distribution.

- Another solution stated by authors of [27] is a probabilistic approach to the pairing process that allows each node in the network to dynamically find a peer and to sync on a (random) available frequency. So, it is a
combination of probabilistic pairing and frequency tuning.

- Hopping across different bands is another solution proposed in [28]. The model treats players as a single secondary user and ‘m’ malicious users, which relies on a Markov decision process. At each stage of the game, the attacker is assumed to be sensing a CRN transmission and creating a PUE attack. Then, the secondary user decides whether to remain at a given channel or to hop, based on the observation of the current and past slots. A learning algorithm is applied to discover the attacker’s strategy and then derive the optimal defense strategy at each step.

- A polynomial based jamming resilient key assignment protocol is proposed by authors of [29]. 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.

- The paper [30] 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 stochastic sum game called jamming resilient control channel (JRCC) is presented in [31]. The game models the interchange among the cognitive radio users and the attacker under the impact of the primary user. Several other jamming detection and prevention techniques have been proposed by Konstantin’s et al [32].

E) DoS Attacks

Denial of Service Attacks (DoS), as the name suggests means denial to spectrum access. If a device never passes the carrier-sensing phase of the CSMA (Carrier Sense Multiple Access) medium access control protocol, then the device is said to be DoS attacked. These attacks can be applicable to both PHY as well as MAC layers. In the MAC layer, a DoS attack is launched through Common Control Channel (CCC).

- A malicious node forces its way to reduce channel utilization by forging MAC control frames, thereby reducing the probability of secondary users finding available channels in the MAC layer i.e. the legitimate users are made to assume that the channel is occupied and they have to delay their data transmission. One such spurious DoS attack affecting the performance of a multi-hop CRN has been demonstrated with simulation results in [33]. On the contrary, in the PHY layer, attacker blocks usage of secondary users by covering the specific spectrum sensing bandwidth with energy i.e. attacker emits energy of the same frequency that is used by other legitimate users. The consequences of such attacks depend on the area of application of ad hoc network and can have many forms [4]:

  - **Centralized classical method** – A centralized resource will be thronged so that it finally crashes and fails in its service operation.
  - **Distributed method** – The attackers possess an adequate computing power and bandwidth which can very easily crash the smaller ad hoc networks.

DoS attacks executed through Channel Eviction Triggering (CET) can be classified as CET and CET-Jamming attacks [34]. In the case of the former, the truthful CRs will need to be denied access to the licensed bands by the adversary CRs. In the latter case, adversary nodes deny communication chances of CRN over the primary bands.

The authors of [35] proposed a prediction based DoS attack defense mechanism, assuming that some compromised grid devices launch DoS attack in a distributed fashion by frequently sending false data or authentication requests along the network hierarchy. [36] uses a Gaussian process, collects reports/observations to form the prior beliefs of the Gaussian process. Using these prior beliefs and observations, posterior probability distributions of the Gaussian process is calculated. The optimal parameters of the Gaussian process are obtained by maximizing the log likelihood of the training data with respect to the parameters. Decision can be taken about the occurrence of a DoS attack and send warning signals to the device bound to be attacked.

The authors in [37] propose a Quickest Detection of Denial-of-Service Attacks algorithm in Cognitive Wireless Networks, which is a non-parametric version of the Pages cumulative sum (CUSUM) algorithm in order to minimize the detection delay so that a network manager may react to the event as soon as possible to mitigate the effect of the attacks. Reservation based DoS attacks are countered in [38] by using a new control packet CTSR.

F) Continuous Channel Access (CCA) Attacks

When a malicious node continuously floods the MAC protocol with continuous transmissions are requests for receptions, the other nodes waiting for channel access end up in starvation.
The probable solutions to such attacks are Time-division multiplexing of each node competing for channel access and Rate Limiting wherein additional, repetitive requests are ignored by the channel.

G) Congestion/Collision Attacks
Attacker engulf the CCC to extend DoS attacks. This is very much similar to the continuous channel access attack [39]. The simple understanding of collision goes with multiple nodes attempting simultaneous transmission on the same channel. A malicious node does not follow the MAC protocol rules and causes collisions with neighboring nodes’ transmissions by sending a short noise packet. On collision, data corruption is guaranteed, causing a checksum mismatch at the receiving end, terming the received data packet as invalid. These attacks do not consume more energy of the attackers, hence simplifying the malicious job of the attacker nodes. Ideally, the usage of error-correction codes seeks to defend such attacks.

H) Unintelligent Replay Attacks
The author in [40] extracts information regarding the unintelligent replay attack, wherein the attacker does not have any understanding of the MAC protocol. A malicious node replicates old control messages that have been intercepted earlier. Valid nodes use this expired topology data and update their routing causing an erroneous view of the network topology.

Here, a lot of energy is wasted in the process of transmission and reception of extra data packets since the recorded events are replayed into the networking, thereby preventing the nodes from going to sleep state. The replaying of events definitely poses serious effects on network performance. These attacks can be prevented only if nodes are supported by anti-replay mechanisms.

I) Unauthenticated Broadcast Attacks
In an unauthenticated broadcast attack, the attacker completely understands the MAC protocol but does not have the capability to penetrate the network; same is the case of Intelligent Jamming Attacks which can in fact differentiate between data traffic and control traffic. The attacker broadcasts the unauthenticated traffic into the network by following all MAC rules. Energy consumption increases since most of the nodes will be forced to stay in listen mode, may be even for extended time durations. Studies reveal that possibilities of such attacks are more in short messages with short adaptive timeout period.

J) Full Domination Attacks
In this kind of an attack, the attacker is fully aware of the MAC protocol and can also penetrate through the network. Studies reveal that almost all kinds of MAC layer protocols are vulnerable to this kind of attack. Network efficiency is reduced by introduction of authenticated broadcast and replaying messages.

K) Exhaustion Attacks
Exhaustion attacks are similar to full domination attacks in the perspective that attacker is fully aware of the MAC protocol and can also penetrate through the network. The difference being that RTS (Request to Send) and CTS (Clear to Send) based MAC protocols are prone to such attacks. Energy of nodes get drained out excessively due to unavailable sleep time. Malicious nodes continuously transmit RTS to nodes, getting CTS acknowledgements as confirmation. All the neighbours of the sender and receiver update their NAV field with the overhearing time during transmission. The immediately arising problem is that even the attacker in the local neighborhood is aware of the duration of the ongoing transmission and may attempt to transmit a few bits within this period to incur bit errors in a victim’s link layer frame via wireless interference [41].

Ways to handle this attack include, channel monitoring and data retransmission mechanism, setting competitive thresholds [42]. Restricting the transmission speed of the network, forces the sensor nodes to automatically abandon the redundant data. However, deterioration in network efficiency is a disadvantage in this method. In [43], the authors have presented a model of exhaustion attack and a pattern recognition based way to devise and detect the attack.

L) Back-Off Attacks
An attacker causes severe performance degradation by minimizing the CW min and thus his back-off period [44]. Back-off attacks and the Sensed Data Privacy Attacks are Cognitive Wireless Sensor Network (CWSN) attacks. Authors of [45] propose a theoretical framework for detecting misbehaving nodes that deviate from the back off mechanism. The detection problem is formulated within a min max robust detection, the Sequential Probability Ratio Test (SPRT).

M) Sensed Data Privacy Attacks
These attacks typically occur in distributed sensor networks and in both physical and link layers. The attacker’s leaves/ drop the channel and analyse the traffic in order to intercept the sensed data transmitted by the sensors.

N) Control Channel Saturation DoS (CCSD) Attacks
A distributed channel negotiation process is initiated between the CRs of a multi-hop CRN. Since there is a limit on the number of concurrent data channels that can be serviced by a single channel, managing multiple CR communication with a common control channel becomes a bottleneck. The MAC control frames are exchanged for channel reservation during the channel negotiation phase. This CCS attack works only on multi-hop CRNs. The reason why it fails to attack the centralized CRNs is that all MAC
frames in a centralized CRN are strictly authenticated by the base station and cannot be easily forged. The control channel will be in a saturated mode once it is not able to carry more control traffic. An attacker can broadcast a large number of packets with the intent to saturate the control channel. When an attacker forces the network with forged MAC control frames, the control channel gets saturated, number of link layer collisions increase thereby deteriorating the network performance. Detection mechanism of CCSD attacks as well as Selfish Channel Negotiation Detection (SCND) attacks discussed in the next subtitle is based on trust [46]. The suggested countermeasure adapts a trusted architecture where any suspicious CR host will be monitored and evaluated by its neighbours. A neighbour can then perform Sequential Probability Ratio Test to reach a final decision whether it is misbehaving or not. Its performance is proven to be good. Authors of [47] propose dynamic channelization where they define an atomic channel as a basic unit of say ‘x’ Hz. Upon the event of control channel migration, a composite channel is formed from the atomic channels, centered around a new carrier frequency.

An alternative decision making strategy based on rendezvous negotiation promises to control the control channel problem [48]. When the common control channel usage approaches the point at which additional allotment of resources is demanded, saturation condition is initiated and the network moves to the phase of rendezvous channel negotiation. This method ensures early channel analysis and start of negotiation prevents the waste of data transmission resources while the common control channel is saturated. Clustering is one other solution to this attack. In each cluster, a common control channel is used. If this control channel is targeted, the other clusters’ nodes will not be affected; hence the affected network area is reduced [49].

O) Selfish Channel Negotiation Attacks

The SCN attack also affects MAC behavior of CR devices. If a CR host retains its energy to increase its own throughput instead of forwarding the data to other hosts, selfish channel concealment results. This may also results in denial of services for users of network for channel negotiation. The detection mechanism to handle this kind of an attack is also based on trust. In fact, the same counter measure suggested for CCSD attack works for this attack too. Malicious nodes can jam the CTS (clear-to-send) signal after receiving the RTS (ready-to-send) signal. The jamming process can complete in the slot time allotted by the 3-handshake exchange of the MAC protocol. The basic idea for any solution for a SCN attack would be to them the selfish nodes a smaller portion of bandwidth or none at all. The authors of [50], describe a cooperative spectrum sensing process modeled as an N-player non-cooperative, non-zero-sum repeated game. Grim Trigger and Carrot-and-Stick are strategies proposed. In Grim Trigger, cooperation from each node is measured and all nodes stop cooperation whenever deviation from any node is detected. This technique does not perform well when channel errors are massive. On the other hand, Carrot-and-Stick is an iterative approach where, at each step, a given node onl y cooperates if all nodes are cooperated or deviated in the previous step. This approach recovers cooperation when all nodes deviate at the risk of leaving the CRN with no information about spectrum availability.

DOMINO (Detection Of greedy behavior in the MAC layer of IEEE 802.11 Networks) is a widely known selfish behavior detection system for WLANs [51]. The authors of [52] propose a scheme that can detect a user that tries to access the channel more often by deviating from the standard exponential back - off mechanism.

P) Biased Utility Attacks

A malicious SU may intentionally tweak parameters of the utility function to increase its bandwidth (in terms of transmission power) [53]. Undetected anomalous behavior may reduce the probability of secondary users and/or base stations getting a fair share of the transmission medium; some users may not even be able to transmit. The authors in [54] put forward a constraint encountered – interference temperature due to secondary transmissions on the primary receivers is below a given threshold.

Q) Asynchronous Sensing Attacks

During normal sensing operations, the main objective is to synchronize sensing activity with other SUs. But, a malicious SU might start transmitting asynchronously which may be misunderstood as PU transmissions leading to missed opportunities.

R) False Feedback Attacks

In CRNs, false feedback from one or a group of malicious user could make other SUs take inappropriate action and violate the terms of the protocol. Such attacks are possible in both centralized as well as de-centralized CRNs. The existing proposals rely on fusion schemes capable of detecting anomalies in the reported sensing data to discriminate malicious validated users. The authors in [55] provided the first fusion-based detection scheme and used the likelihood ratio as decision variable. But, the disadvantage of this method was that a a priori knowledge of the probabilities is required, which may be unknown to the CRN.
In [56], a Weighted Sequential Probability Ratio Test (WSPRT) was proposed, an extension to the previous proposal. This is a reputation-based mechanism. Initially, each node’s reputation is updated, initially zero, and incremented or decremented by one whenever the local sensing report is consistent with the final decision. Other reputation schemes are presented in [57], proposed a simple model where the reputation degree of secondary users is set to 0, 0.5 or 1. When the report provided by a given secondary user matches the final decision, the reputation degree is increased by 0.5 else decreased by 0.5.

In [58], a reputation system is proposed where initially the trust value for a given node is computed by taking into account its past. A forgetting factor is applied in order to give higher weights to recent behaviours and gradually decrease the influence of older ones. OSRP (On-demand Secure Routing Protocol) is a reputation-based protocol. In [59], a WSPRT hypothesis test is also used as data fusion scheme, but the weights assigned to each node are computed according to its statistical importance based on a shadowing correlation model applied to a two-dimensional area. Finally, in [60] and [61], different schemes for detecting malicious users based on outlier’s detection have been evaluated. The authors of [60] bring out an outliers factor is assigned to each secondary user at the kth sensing iteration by using the sample mean and the sample standard deviation of the reported energy values In statistics, an outliers is an observation that is numerically distant from the rest of the data. The technique in [61] does not perform well when the distribution of the energy values is highly skewed. In such case, valid values lying on the heavy-tailed side of the distribution will be assigned a high outliers factor, meaning that they will have a very low impact on the final decision.

Other techniques based on other statistical parameters such as the Median Absolute Deviation (MAD) or the Bi-Weight Scale (BWS), which are shown to be more robust.

S) Fabrication Attacks
A malicious SU deliberately reports inverted sensing results to a SU base-station (SUBS) all the time and causes deterioration to the overall performance of all the CRNs [58]. These attacks either prevent other SUs from accessing network resources or introduce excessive interference to PU spectrum bands.

T) Byzantine Attacks
This attack is also known as spectrum sensing data falsification (SSDF) attacks. Attacker sends false information about spectrum sensing to its neighbours, the neighbours falsely think that there are no free spectrum bands available so they move away from that place, malicious can occupy the spectrum. Such attacks affect the distributed CRNs where there is mutual cooperation between the CRNs. Whereas, CRNs in centralized networks are less affected. However, centralized CRNs also cannot escape Byzantine attacks when some DBMS issues surrounding the centralized data arise. There exist multiple ways [62] in which a Byzantine attack can be triggered;

(a) Denial SSDF - Fusion center gets false information that a channel has been occupied and concludes that a PU is present.
(b) Induce SSDF - On the contrary, false information about a channel being unoccupied can cause interference to working, authenticated PUs which have authenticated occupancy in that channel.
(c) Sybil-based SSDF – Malicious nodes pose an impression that they will provide the required sensing functionalities and legitimate nodes rely on such false-promising nodes and communicate valuable information to them. Some solutions include [63]:

- Decision fusion technique: where all collected local spectrum-sensing results are summed and compared to a threshold to detect an attack. Using fixed thresholds is a drawback in a scenario of multiple attackers, but varying the threshold damages the threshold decision.
- Weighted Sequential Ratio Test: Solution includes a reputation maintenance step and the actual hypothesis test.
- Weight based fusion scheme: Uses trust approach and pre-filtering techniques.
- Detection mechanism that runs in the fusion center: The fusion center identifies and eliminates attackers from the data fusion process. Only works when a centralized fusion center exists.
- Detection mechanism that requires a priori knowledge: Prior information is mandatory but is not reliable information one can get from a network.
- Neyman-Pearson Test: Here, a maximum acceptable probability of miss detection is defined.
- Detection mechanism based on trust: A trust framework consisting of a Trust Policy Engine and a Trust Metrics Engine is proposed in [64]. A trust level is determined based on past behavior and impact on the performance of the network. The major drawback is that the scheme cannot be applied to multiple malicious users’ scenario. Some of the schemes/algorithms proposed are [65]:

www.gjaet.com
Trust can also be assigned based on context. A trust based authentication system has been proposed in [66]. Reputation based detection forms the basis of many schemes to identify malicious nodes [70, 71, 72, 73]. A reputation measure representing the number of times the local decision of a node can differ from the global decision of the fusion center in a time window is assigned to each node. The higher the value of the measure, the less reliable the node’s observation. 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.

A trust based authentication system has been proposed in [74], where node with the highest level of trust is appointed as the base station. Each node shares a unique key with the base station. In the certificate based trust authentication technique, base station generates trust values for each node. Trust values are typically 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. Base station updates the node with updated trust value each time the base station sends a broadcast message.

Trust can also be assigned based on context (time, location, spectrum, code, and Angle), sensing evidence scope and importance and lastly a time window [75]. This 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 [76] depends 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 the algorithm. The node’s ability to access the network resources is based upon the trust determination.

Another trust metric named Location Reliability and Malicious Intention (LRMI) has been considered in [77] which reflects path controls characteristics of wireless channels. Evaluation of sensing reports sent to the fusion center is the report sending cell (Location Reliability) as well as the report generator (Malicious Intention). A trust value is applied to each cell based on the activity of the cell members. The algorithmic combination of the two values help to alleviate the trust devaluation that generally occurs due to a node’s signal path loss because of its location and mobility, hence providing a more accurate trust determination strategy.

Detection using two conditional frequency check statistics (CFC) is presented in [78] where two constraints are enforced 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.

Authors of [79, 80] propose statistically based analysis schemes to detect malicious users and alleviate the false sensing observations. [79] Allows for an unknown number of malicious cognitive radios in a network, keeping in mind that any node can suddenly turn malicious. 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. [80] 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 outperforms the Grubbs’s test and the box plot test in detecting the presence of a single bad actor. 

- The authors of [81] use a statistical attack model to identify malicious nodes using Bayesian approach. The algorithm estimates the channel status and probabilities of attacks to identify the Byzantines. Belief propagation is used with factor graphs to solve the Bayesian estimation problem.

- A primary user’s received signal strength (RSS) is the base determining factor in [82]. This method is proved to work irrespective of the ratio of legitimate and false nodes. Signal strength of primary user’s receiver determines its location with respect to a secondary user and reports the same data to the fusion center. The algorithm compares this location with that calculated using the combined data from the network secondary users at the fusion center. This comparison is used to check whether data provided by the secondary user true or false.

- An indirect punishment based mitigation scheme is presented in [83]. If the primary user encounters any collision, it applies punishment to the entire network.

- The authors of [84] present a payment based solution wherein the node refuses to forward packets over free channels. Only when the node offers a free channel to forward the packets, node will get the payment. A transmitting node will also pay a neighbour for packet transmission over a channel when that neighbour’s services are required for transmission. A central authority is required to maintain the credit balance for each node and this is an overhead requirement for the nodes.

V. LINK LAYER ATTACK DETECTION AND SOLUTION SCHEMES

The authors in [85] present an anomaly-based algorithm which considers the ratio of the corrupted packets over the correctly decoded packets as the metric that reveals jamming when the attacker’s energy is emitted on the same channel. MAC Spoofing attacks can be detected by Gaussian mixture model based approach [86] wherein an address is determined to be MAC spoofed based on the received signal strengths. Specific attacks targeting Wireless Sensor Network (WSN) protocols like S-MAC, B-MAC and L-MAC are discussed in [87]. As a solution, high duty cycle is suggested for S-MAC and shorter data packets for L-MAC. A cumulative sum non-parametric algorithm that considers the back-off value of genuine contenders handles link layer mis behavior [88]. Another algorithm proposed in [89] utilizes the sequence number field carried by the data packets. The sequence numbers of each frame from a common source node is recorded. An abnormal frame gets recorded once there arises a gap between current sequence number and the last recorded frame. A Signature based Authentication Coded Intrusion Detection Scheme [48] is a new proposal that detects the Byzantine attack. It works in asynchronous systems like Internet and incorporates optimization to improve detection response time. TABLE I summarizes the Link layer and MAC layer attacks, the detection techniques, possible countermeasures and proposed algorithms.

VI. CONCLUSION

Cognitive Radio Networks are basically wireless networks which are definitely prone to network threats and attacks. This paper extensively puts forth a discussion about all possible Link layer and MAC layer attacks, detection techniques, possible countermeasures and solution algorithms proposed so far. The proliferation of wireless technology has been remarkable so far and will continue to be even better, but for the increasing threats in parallel. New threats and vulnerabilities will only be on the increasing graph and one has to come up with more and more advanced threat combating algorithms and countermeasures. Any new Link layer or MAC threat proposed along with their countermeasures/ algorithms will stand up as future work for this paper.
<table>
<thead>
<tr>
<th>Threat/Attack</th>
<th>Concepts of Counter Measures/Strategies</th>
<th>Work Reference/Contribution</th>
</tr>
</thead>
</table>
| Beacon Falsification | ➢ Inter-cell key management scheme  
➢ Distributed key management scheme  
➢ Beacon authentication mechanism | Shameek et al.[6] |
| Smaller Back off Window (SBW) attack | ➢ Cumulative distribution function (CDF)-based solution | Toledo et al.[8]  
Wang et al.[9] |
| MAC Spoofing | ➢ Rate Limiting to the MAC admission control protocol for the network to ignore excessive requests.  
➢ Usage of time-division multiplexing where each node is allotted a time slot in which it can transmit.  
➢ Use of extensible authentication protocol (EAP) methods that allow mutual authentication. | Kavitha et al.[39]  
Sheng et al.[86]  
Ma et al.[21] |
| Jamming attacks | ➢ Use of Error Control Codes  
➢ Physical layer defences like directional antennas and spread spectrum  
➢ Link layer defences like Frequency hopping  
➢ Network layer defences like spatial retreat  
➢ Machine learning/game theory-based approaches  
➢ Dynamic Common Control Channel (CCC) allocation and Key distribution  
➢ Combination of probabilistic pairing and frequency tuning  
➢ Anomaly detection approach to profile the CRN system parameters through a learning phase  
➢ Frequency hopping with pseudo-random channel switching  
➢ A rapid frequency hopping scheme to avoid narrow-band jamming | Kavitha et al.[39]  
Alfred et al.[20]  
Fragkiadakis et al.[85]  
Lazos et al.[22]  
Tague et al.[25]  
Wu et al.[19]  
Shoham et al.[15]  
Wang et al.[17]  
Zhang et al.[12]  
Wu et al.[13]  
Wang et al.[90]  
Roberto et al.[27]  
Zubair et al.[91]  
Navda et al.[23]  
Gummadi et al.[24] |
| DoS Attacks | ➢ Usage of small frames to ensure that channel is seized for a smaller duration only  
➢ Minimization of detection delay to ensure immediate reaction of the network manager to mitigate the effect of the attacks  
➢ Prediction based DoS attack defence mechanism, assuming that some compromised grid devices launch DoS attack distributed by frequently sending false data or authentication requests along the network hierarchy  
➢ Reports/observations from the prior beliefs of the Gaussian process, using which, posterior probability distributions of the Gaussian process is calculated.  
➢ Use of CTSR control packet | Kavitha et al.[39]  
CaLynna et al.[37]  
Fadlullah et al.[35]  
Xu Li et al.[36]  
Negi et al.[38] |
| Continuous Channel Access (CCA) attacks | ➢ Time-division multiplexing of each node competing for channel access  
➢ Rate Limiting wherein additional, repetitive requests are ignored by the channel | |
<p>| Congestion attacks | ➢ Use of Error Control Codes | Kavitha et al.[39] |
| Unintelligent Replay Attack | ➢ Anti-replay mechanisms for nodes. | |
| Unauthorized Broadcast Attacks | ➢ Ensuring longer messages with prolonged adaptive timeout period. | |</p>
<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Description</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Domination Attack</td>
<td>Strong link layer encryption in deployed sensor networks</td>
<td>Fangmin et al.[42]</td>
</tr>
<tr>
<td></td>
<td>Cluster-based MAC protocols and secure slot assignment</td>
<td>Baig et al.[43]</td>
</tr>
<tr>
<td>Exhaustion attacks</td>
<td>Setting competitive threshold</td>
<td></td>
</tr>
<tr>
<td>Back-off Attacks</td>
<td>Cumulative sum non-parametric algorithm</td>
<td>Cardenas et al.[88]</td>
</tr>
<tr>
<td></td>
<td>Method utilizing the sequence number field carried by the data packets. The sequence numbers of each frame from a common source node is recorded.</td>
<td>Guo et al.[89]</td>
</tr>
<tr>
<td></td>
<td>Scheme that can detect a user that tries to access the channel more often by deviating from the standard exponential back-off mechanism</td>
<td>Kyasanur et al.[52]</td>
</tr>
<tr>
<td>Control Channel Saturation DoS (CCSD) Attack</td>
<td>Implementation of a trusted architecture where the neighbour performs Sequential Probability Ratio Test to reach a final decision whether the malicious CR is misbehaving or not.</td>
<td>Wenkai et al.[46]</td>
</tr>
<tr>
<td>Selfish Channel Negotiation</td>
<td>Detection based on trust, same as for CCSD</td>
<td>Wenkai et al.[46]</td>
</tr>
<tr>
<td>Biased Utility</td>
<td>Constraint encountered solutions for secondary transmissions on primary receivers based on a particular threshold value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trust management on secondary users for resource hungry and collaborative trust</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management of systems objective function by controlling the radio parameters</td>
<td></td>
</tr>
<tr>
<td>False Feedback attacks</td>
<td>A Fusion-based detection scheme using likelihood ratio as decision variable</td>
<td>Ruiliang et al.[55]</td>
</tr>
<tr>
<td></td>
<td>Weighted Sequential Probability Ratio Test (WSPRT) - reputation-based mechanism</td>
<td>Chen et al.[56]</td>
</tr>
<tr>
<td></td>
<td>Simple model where the reputation degree of secondary users is set to 0, 0.5 or 1</td>
<td>Chen et al.[57]</td>
</tr>
<tr>
<td></td>
<td>Reputation system where initially the trust value for a given node is computed by taking into account its past.</td>
<td>Qin et al.[58]</td>
</tr>
<tr>
<td></td>
<td>WSPRT hypothesis test where weights assigned to each node are computed according to its statistical importance based on a shadowing correlation model applied to a two-dimensional area</td>
<td>Min et al.[59]</td>
</tr>
<tr>
<td></td>
<td>An outliers factor is assigned to each secondary user at the kth sensing iteration by using the sample mean and the sample standard deviation of the reported energy values in statistics.</td>
<td>Praveen et al.[60]</td>
</tr>
<tr>
<td></td>
<td>Valid values lying on the heavy-tailed side of the distribution will be assigned a high outliers factor</td>
<td>Kaligineedi et al.[61]</td>
</tr>
<tr>
<td>Fabrication Attacks</td>
<td>Verification of reports in a deterministic and hop-by-hop fashion</td>
<td>Tague et al.[26]</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Signature based Authentication Coded Intrusion Detection Scheme to detect the Byzantine attack [future]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision fusion technique where all collected local spectrum-sensing results are summed and compared to a threshold to detect an attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weighted Sequential Ratio Test where solution includes a reputation maintenance step and the actual hypothesis test.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight based fusion scheme uses trust approach and pre-filtering techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection mechanism that runs in the fusion center identifies and eliminates attackers from the data fusion process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection mechanism with priori knowledge where prior information is mandatory but is not reliable information one can get from a network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neyman-Pearson Test where a maximum acceptable probability of miss Detection is defined.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pinokio method of detection of Byzantines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooperative neighbouring cognitive radio nodes (COOPON) method of detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database of valid data acts as a trusted data source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Based on differing signal energy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation based detection scheme</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust based authentication system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust assigned based on context (time, location, spectrum, code, and Angle), sensing evidence scope and importance and lastly a time window</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct trust calculation is based on a cumulative attribute determined by the success or failure of past requests, responses, and retransmissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A trust metric named Location Reliability , and Malicious Intention (LRMI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection using two conditional frequency check statistics (CFC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A statistically based analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A statistical attack model using Bayesian approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Based on primary user’s received signal strength (RSS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An indirect punishment based mitigation scheme</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A payment based solution wherein the node refuses to forward packets over free channels</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REFERENCES


[36] Xu Li, Inria Lille, Xiaohui Liang, Rongxing Lu, and Xuemin Shen, “Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges,” CYBER SECURITY FOR SMART GRID COMMUNICATIONS.


www.gjaet.com

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


