International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Survey on Data Fusion and Security Threats in CR Networks

Anita Sharma[Á*], Swarn Ahuja[Á] and Moin Uddin[B]

[Á]Department of Electrical, Electronics and Communication Engineering, ITM University
[B]Department of Electrical Engineering, Jamia Islamia University

Accepted 20 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

For cognitive radio networks, it has been proven that cooperative spectrum sensing is more reliable and efficient as far as detecting spectrum holes in cognitive radio networks (CRNs) is concerned. It does this by combining sensing information of multiple cognitive radio users. Cooperative spectrum sensing has been known to greatly improve the detection range and capability through exploitation of the inherent spatial diversity in cooperative relaying strategies. In implementing cooperative relay based energy detection, data fusion and decision fusion are the two major approaches have been identified in literature. Although the notion of cooperative relay based data fusion has been well discussed in literature, in this paper, we study different aspects of fusion and the different schemes that can be implemented in fusion center. Also a brief introduction about malicious attacks that a cooperative cognitive radio network can suffer from and methods to combat them are given at the end of the paper.

Keywords: *Cooperative spectrum sensing, cognitive radio network (CRN), data fusion, soft, quantized and hard fusion rules, denial of service (DoS), incumbent emulation(IE) or primary user emulation attack(PUEA), security, spectrum sensing data falsification(SSDF)*

1. Introduction

Proper spectrum sensing is the key to identifying the available spectrum in cognitive radio networks and prevent the harmful interference with licensed users .

However there is a possibility of sharing spectrum among different parties subject to interference-protection constraints. There can be spectrum-sharing between a primary licensee and a group of secondary users. In order to enable access to unused licensed spectrum, a secondary user has to continuously monitor licensed bands and opportunistically transmit whenever primary signal is not detected. However, detection performance in practice is often compromised with multipath fading, shadowing and receiver uncertainty issues. To mitigate the impact of these issues, cooperative spectrum sensing has been shown (I.F.Akyildiz *et al,2011*;A. Ghasemi *et al*,2005; S. Mishra *et al,2006;* C.Sun *et al,2007)* to be an effective method to improve the detection performance by using spatial diversity. This results in cooperative gain such as improved detection performance and relaxed sensitivity requirement though at the cost of cooperation overhead. The overhead will be in terms of any extra sensing time, delay, energy and operations devoted to cooperative sensing and can even lead to performance degradation at times. But the advantages of cooperative gain far outweigh the problems due to cooperative overheads. Broadly the cooperation method is analyzed by the fundamental components called the elements of cooperative sensing, which includes cooperation models, sensing techniques, hypothesis testing, data fusion, control channel and reporting, user selection, and knowledge base (I.F.Akyildiz *et al,2011*). As are the incurred cooperation overheads like the sensing time and delay, channel impairments, energy efficiency, cooperation efficiency, mobility, security, and wideband sensing issues.

2. Cooperative Spectrum Sensing and Energy Detectio

Although there exist different methods of spectrum sensing, we will be using energy detection primarily due to its simplicity.

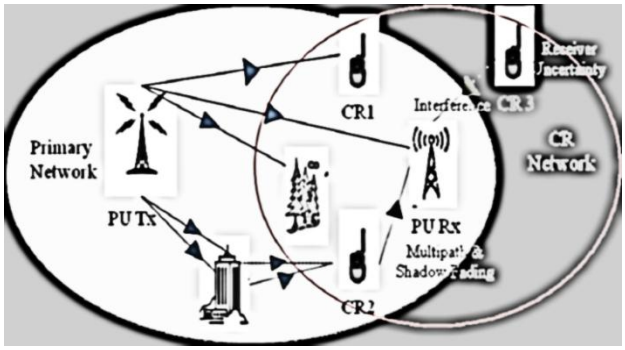

Fig1: Problems due to shadowing and multipath

*Corresponding author: **Anita Sharma**

Its biggest limitation though is that it does not work satisfactorily when SNR is low. In cooperative spectrum sensing each CR performs spectrum sensing individually called local sensing.

Typically, local sensing for primary signal detection can be formulated as a binary hypothesis problem as follows (I.F. Akyildiz *et al*,2009):

$$x_k(n) = w_k(n) \quad H0 \qquad (1)$$
$$h_k(n).s(n) + w_k(n) \quad H1 \qquad (2)$$

where k is the number of cognitive users in the network (indexed by k = {1, 2. . . K}),$x_k(n)$ denotes the received signal at the CR user, s(n) denotes the samples of the transmitted PU signal, $h_k(t)$ is the channel gain of the sensing channel, w_k (n) is the zero-mean additive white Gaussian noise (AWGN), H_0 and H_1 denote the hypothesis of the absence and the presence, respectively, of the PU signal in the frequency band of interest. For the evaluation of the detection performance, the probabilities of detection $P_{d,k}$ and false alarm $P_{f,k}$ are defined as

$$P_{d,k} = P\{\text{decision} = H_1|H_1\} = P\{Y > \lambda \mid H_1\} \qquad (3)$$
$$P_{f,k} = P\{\text{decision} = H_1|H_0\} = P\{Y > \lambda \mid H_0\} \qquad (4)$$

Where Y is the decision statistic and λ is the decision threshold. The threshold is set depending on the requirements of detection performance. Based on these definitions, the probability of a miss or miss detection is defined as

$$P_{m,k} = 1 - P_{d,k} = P\{\text{decision} = H0|H1\}. \qquad (5)$$

The metric for the performance evaluation of sensing techniques is demonstrated by a plot of $P_{d,k}$ versus $P_{f,k}$ and is called the receiver operating characteristic (ROC).

There is another added benefit of cooperative sensing. Due to multipath fading and shadowing, the signal-to-noise ratio (SNR) of the received primary signal can be extremely small and its detection becomes a difficult task. Since receiver sensitivity indicates the capability of detecting weak signals, the receiver will have a strict sensitivity requirement greatly increasing the implementation complexity and the associated hardware cost. More importantly, the detection performance cannot be improved by increasing the receiver sensitivity, when the SNR of PU signals is below a certain level known as a SNR wall. The sensitivity requirement and the hardware limitation issues are considerably relieved by cooperative sensing. Fig. 1 shows that the performance degradation due to multipath fading and shadowing can be mitigated by cooperative sensing so that the receiver's sensitivity can be approximately set to the level of nominal path loss without increasing the implementation cost of CR. To get a better understanding of the problem, consider this: a typical Digital TV receiver operating in a 6MHz band should be able to decode a signal level of at least -83dBm without significant errors (Longley-Rice Methodology,2004). If the typical thermal noise in such bands is -106dBm. Hence a CR which is 30dB more sensitive will be able to detect a signal level of -113dBm, which is below the noise floor.

Based on the logic discussed above, our model of the radio is simple: considering a threshold for the received signal strength λ, the radio declares that the Primary user is present if and only if the received signal strength RSS is greater than λ. To meet the detection target $P_{d,k}$ it is necessary that the received signal strength exceeds λ even in the worst case when $P_{d,k}$ is severely affected by the fades. Since cooperation makes $P_{d,k}$ closer to zero, the system as a whole becomes robust to the effects of the fading environment.

Although there are quite a few cooperation models existing, we will be working with parallel fusion model in this paper. It is similar to distributed detection and data fusion where (P.K. Varshney,1997) a group of spatially distributed sensors observes a physical phenomenon H (hypothesis testing parameter) through the observations y_i , through the sensing channel and report their observations u_i to a central processor known as a FC (R. Viswanathan *et al,1997)* through the reporting channel. The FC combines the reported data by data fusion using one of the data fusion rules and makes the global decision *u* by using binary hypothesis testing. Fig. 2. Typically depicts this fusion model.

There are a few factors which need to be considered before cooperative sensing can be implemented and common control channel (CCC) being the most important one of those.

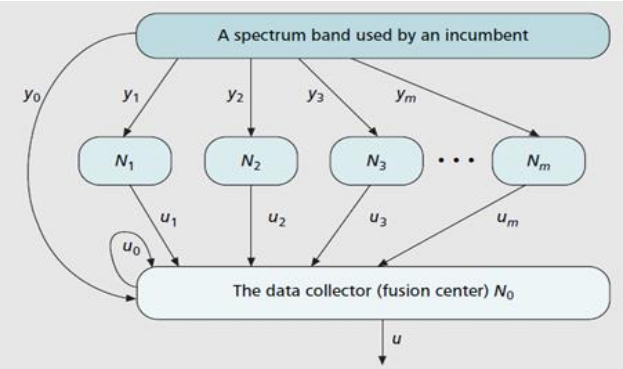

Fig. 2: Parallel Fusion Network

Common Control Channel (CCC) : The common control channel (CCC) in cooperative sensing in CR, is commonly used by users to report local sensing data to the FC and to share the sensing results with neighboring nodes. Hence a control channel is an important element of cooperative spectrum sensing. The control channel can be implemented as a dedicated channel in licensed or unlicensed bands, or an underlay ultra-wideband (UWB) channel (D. Cabric *et al* , 2004). All the cooperating CR users access the control channel by using a MAC scheme for multiple access . A physical point-to-point link from a cooperating CR user to the FC is called a reporting channel. Three major control channel requirements of bandwidth, reliability, and security must be satisfied by a control channel to act as a trustworthy reporting channel
The bandwidth of the control channel is identified in (S. Mishra *et al,2006)* as one of the most important factors

in determining the level of cooperation. This is is limited by The control channel bandwidth can limit the amount of local sensing data that can be transmitted to the FC or shared with the neighbors. The control channel bandwidth constraints are addressed by censoring and quantizing local sensing data as discussed in (C. Sun *et al*,2007). Censoring is performed by each user by reporting the result only if the local decision is determined by the sequential probability ratio test or SPRT. Thus, censoring limits the unnecessary reporting and the usage of control channel bandwidth. (X. Zhou *et al*,2010) proposes a bandwidth efficient combination scheme to enable the simultaneous reporting to the FC with the fixed required control channel bandwidth irrespective of the number of CR users. The test statistics are devised for Gaussian and Rayleigh fading reporting channels.

Apart from bandwidth, reliability of the control channel has the great impact on cooperative sensing performance. The control channel is susceptible to multipath fading and shadowing like data channels. The reliability issue of the control channel needs to consider the channel impairments too. Assumption of a perfect error-free control channel in cooperative sensing in early studies (A. Ghasemi *et al*,2005*)* was gradually proven wrong when recent studies investigated the effect of Gaussian noise (Z. Quan *et al*,2008), multipath fading (W. Zhang *et al* ,2008), and correlated shadowing (M. Di Renzo *et al*,2009) on the control channel. Performance degradation caused by reporting channels under fading was addressed by a transmit diversity-based cooperative sensing method in (W. Zhang *et al* ,2008). It is shown in (W. Zhang *et al* ,2008) that reporting errors can cause the results to show that the probability of false alarm P_f is lower bounded and linearly increases with the probability of reporting errors. Also results from unreliable reporting channels are censored in censor-and-relay method proposed for the FC . The CR users not having good reporting channels are instructed to forward their sensing results to the neighbors having good reporting channels. These neighbors then report all the results through orthogonal control channels to avoid the mutual interference.(M. Di Renzo *et al*,2009), investigates the issue of correlated log-normal shadowing on the reporting channel. The results show that the performance degradation on the reporting channel and the sensing channel caused by the shadowing correlation is more or less similar.

3. Spectrum Sensing Techniques

Cooperative spectrum sensing is characterized by the following three techniques:

1. Centralized Techniques
2. Distributed/decentralized Techniques
3. Relay-assisted Techniques

Centralized Techniques: It is the fusion center,FC, in centralized cooperative sensing, that controls the three-step process of cooperative sensing. The FC first, selects a channel or a frequency band of interest for sensing and then instructs all cooperating CRs to individually perform local sensing. All cooperating CR users then report their sensing results to the FC via the control channel. The FC, after receiving the sensing information from all the CRs, combines the information, determines the presence of PUs, and diffuses the decision back to cooperating CR users as shown in Fig. 3. All CR users are tuned to the selected licensed channel or frequency band for local sensing, and the physical point-to-point link between the PU transmitter and each cooperating CR user for observing the primary signal is called a sensing channel. All CR users are tuned to a control channel for data reporting. The reporting channel is the physical point-to-point link between each cooperating CR user and the FC for sending the sensing results.

However the centralized cooperative sensing can occur in either centralized or distributed CR networks. In centralized CR networks, a CR base station (BS) acts as the FC whereas, in CR

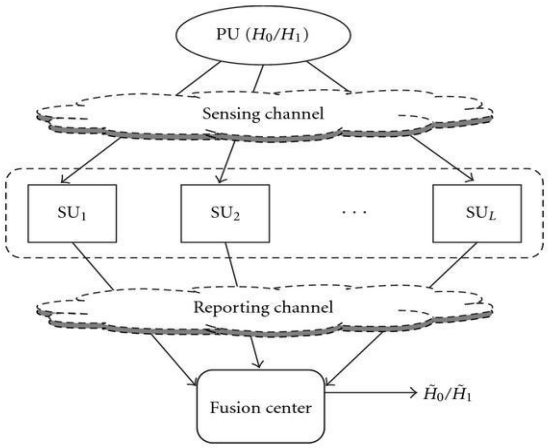

Fig 3: Centralized data fusion

ad hoc networks (CRAHNs),as the CR BS is not present, any CR user can act as a FC to coordinate cooperative sensing and combine the sensing information from its peers.

Distributed/Decentralized Techniques: Decentralized /distributed cooperative sensing does not rely on a FC for making the cooperative decision. Here the CR users communicate among themselves and converge to a unified decision on the presence or absence of PUs by iterations.

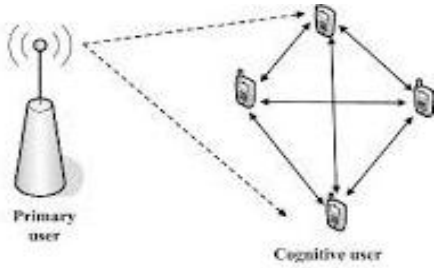

Fig 4: Decentralized Cooperative Sensing

Fig.4 illustrates the distributed/decentralized cooperative sensing. After local sensing, CRs share the local sensing

results with other users in their vicinity. Based on a distributed algorithm, each CR user sends its own sensing data to other users and by using a local criterion, combines its data with the received sensing data from other CRs, and decides about the presence of PU. If the criterion is not satisfied, CR users send their combined results to other users again and repeat this process until the algorithm converges and a they reach a decision. Hence a distributed scheme may take several iterations to reach the unanimous cooperative decision.

Relay Assisted Techniques: In relay-assisted cooperative sensing, we work on the fact that since both sensing channel and reporting channel are not perfect, a CR user observing a weak sensing channel and a strong report channel and a CR user with a strong sensing channel and a weak reporting channel, for example, can cooperate with each other to improve the overall performance of cooperative sensing.

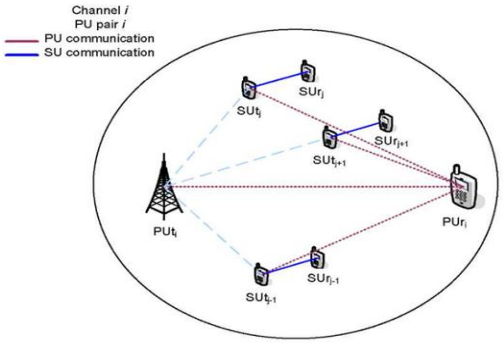

Fig 5: Relay Assisted Cooperative Sensing

As shown in Fig.5 some CRs, may have a strong sensing channel but may suffer from a weak reporting channel. Other nearby CRs, who have a strong reporting channel, may serve as relays to assist in forwarding the sensing results from the first group of CRs to the FC. In this case, these reporting channels can also be called relay channels. The relay-assisted cooperative sensing can exist in both centralized and distributed schemes. In fact, when the sensing results need to be forwarded by multiple hops to the intended receiver node, all the intermediate hops act as relays. Thus, if both centralized and distributed structures are assumed to be one-hop networks, the relay-assisted structure can be considered as multi-hop cooperative sensing. In addition, the relay for cooperative sensing here serves a different purpose from the relays in cooperative communications (K. Ben Letaief *et al*,2009), where the CR relays may be used for forwarding the PU traffic.

In this paper we will use centralized cooperative scheme for the rest of the discussion. As discussed above ,the three steps in the centralized cooperative sensing process, (D. Cabric *et al*, 2004) are :

1- The fusion center FC first selects a channel or a frequency band of interest for sensing and requests all cooperating CR users to individually perform local sensing.
2- All cooperating CR users report their sensing results via the control channel.
3- Then the FC fuses the received local sensing

Information to decide about the presence or absence of primary signal and reports back the decision to the CR users.

Implementation of these three steps involves the following seven elements of cooperative sensing (I.F.Akyildiz *et al,2011)* as illustrated in Fig. 6.

• Cooperation models: this decides how CR users cooperate to perform sensing.
• Sensing techniques: this element is vital in cooperative spectrum sensing to sense primary signals by using signal processing techniques.
• Hypothesis testing: a statistical test is performed to decide about the presence or absence of PU.
• Control channel and reporting: is used by CR users to report sensing results to the FC.
• Data fusion: is a process of combining local sensing data to make cooperation decision.
• User selection: this element provides us the way to optimally select the cooperating CR users in order to maximize the cooperative gain
• Knowledge base: means a prior knowledge including PU and CR user location, PU activity, and models or other information in the aim to facilitate PU detection.

Although there are many methods for primary detection available, energy detection is the simplest to implement. The results though may not be very accurate in case of low SNR but
the simplicity of using energy detection makes it a preferred choice for researchers. The implementation of cooperative relay based energy detection identifies two major approaches: (i) data fusion; and (ii) decision fusion.

There are various rules for combining sensing information from the different CRs and
of these rules, optimum fusion rule is the

Fig 6: Seven steps of cooperative sensing

Chair-Varshney rule which is based on log-*likelihood ratio test (Z. Chair et al, 1986).* Likelihood ratio tests are also used for making decisions from secondary users in (E. Visotsky *et al*,2005; M. Gandetto *et al*,2005; M. Gandetto *et al,2005*;[A. F. Cattoni *et al*, 2006; M. Gandetto *et al,2007)*.There are simpler techniques like equal gain combining, EGC , selection combining, SC and maximum

ratio combining, MRC for combining sensing results as employed in (F. Digham *et al*,2003). The performances of equal gain combining (EGC), selection combining (SC), and switch and stay combining (SSC) are used for energy detector based spectrum sensing when Rayleigh fading channels are used. The EGC method has a gain which is approximately twice in magnitude compared to SC and SSC.

4. System Model

Consider a cognitive radio network, with K users (indexed by $k = \{1, 2. . . K\}$). Spectrum sensing is to be performed to detect the existence of the PU. Suppose that each CR performs local spectrum sensing independently by using N samples of the received signal. The spectrum sensing problem can be formulated as a binary hypothesis testing problem with two possible hypothesis H_0 and H_1 already represented as equations 1 and 2

$$H_0: x_k(n) = w_k(n) \quad (1)$$
$$H_1: x_k(n) = h_k s(n) + w_k(n) \quad (2)$$

where $s(n)$ are samples of the transmitted signal (PU signal), $w_k(n)$ is the receiver noise for the k^{th} CR user, which is assumed to be an i.i.d. random process with zero mean and variance σ_n^2 while h_k is the complex gain of the channel between the PU and the k^{th} CR user. H_0 and H_1 represent absence or presence of the primary signal respectively. Using energy detector, the k^{th} CR user will calculate the received energy as ([V. I. Kostylev, 2002):

$$E_k = \Sigma x_K^2(n) \quad (6)$$

Either each CR user forwards the entire detected energy result E_k to the FC or the CR users make the one-bit decision given by Δ_k, by comparing the received energy E_k with a predefined threshold λ_k.

$\Delta k = \{1,$ for $Ek > \lambda k$
0, Otherwise

Detection probability $P_{d,k}$ and false alarm probability $P_{f,k}$ of the CR user k are as defined in equations 3 and 4 earlier

$$P_{d,k} = P_r\{\Delta_k = 1|H_1\} = P_r\{E_k > \lambda_k|H_1\} \quad (3)$$
$$P_{f,k} = P_r\{\Delta_k = 1|H_0\} = P_r\{E_k > \lambda_k|H_0\} \quad (4)$$

The probability of missed detection is given by:

$$P_{m,k} = 1 - P_{d,k} \quad (5)$$

Fusion decision: There are three fusion rules which the fusion center may use for the fusion decision. They are:
Soft fusion
Hard fusion
Quantized fusion

Soft Fusion : In soft data fusion, CR users forward the entire sensing result E_k to the fusion center without performing any local decision. The FC makes the decision by combining these results by using appropriate combining rules such as square law combining (SLC), maximal ratio combining (MRC), selection combining (SC) and likelihood ratio test(LRT). Soft combination provides better performance than hard combination, but at the same time requires a larger bandwidth for the control channel (V. I. Kostylev, 2002). The overhead generated is also more compared to hard combination scheme (Zhi Quan *et al*, 2008). The combining rule adopted by the FC may be any one of the following:

Square Law Combining (SLC): SLC is one of the simplest linear soft combining rules. Here each node sends its estimated energy to the fusion center where these energies are added together. This summation is then compared to the threshold λ to decide on the presence or absence of the P. The decision statistic is given by (J. Ma *et al*,2007):

$$E_{slc} = \sum_{k=1}^{K} E_k \quad (7)$$

where E_k denotes the energy statistic from the k^{th} CR user.

Maximum Ratio Combining (MRC): The difference between this method and the SLC is that in this method the energy received in the fusion center from each user is multiplied with a normalized weight and then added. The weight depends on the received SNR of the different CR users. The statistical test for this scheme is given by:

$$E_{mrc} = \sum_{k=1}^{K} W_k E_k \quad (8)$$

Selection Combining (SC): In the SC scheme, the fusion center selects the branch with highest SNR.

$$\gamma_{sc} = Max(\gamma_1, \gamma_2, \gamma_3 \ldots \gamma_k) \quad (9)$$

Likelihood Ratio Test (LRT): There is a lot of computational complexity associated with LRT-based fusion methods involving quadratic forms. Therefore (Z. Quan *et al*,2008) proposes an efficient linear combination of local test statistics. Here the local test statistics are weighted by optimized weighting coefficients, optimized for targeted $P_{f,k}$ and $P_{d,k}$ requirements of the CR network. Here a modified deflection coefficient (MDC) is introduced to measure the effect of the PDF on the detector performance as the combining weights affect the PDF of the global statistic,. Simulation results prove better detection probability by maximizing the MDC. This being a heuristic algorithm, significantly reduces the computationally complexity in obtaining the global decision at the cost of slight degradation in the detection performance. Significant performance degradation occurs when the channel noise level increases in optimal linear combination strategy.

Hard decision fusion: In this scheme, each user decides on the presence or absence of the primary user at its end and sends a one bit decision to the data fusion center. The main advantage of this method is its simplicity and the fact

that it needs limited bandwidth (J. Ma *et al*,2007). When binary decisions are reported to the fusion center, it uses any of the three rules of decision, the AND, OR, and MAJORITY RULE. Assume that the individual statistics Δ_k are quantized to one bit with Δ_k= 0, 1; is the hard decision from the k^{th} CR user. 1 indicates that the signal is present, and 0 means otherwise.

The AND decision rule means that a signal is present if all users have detected a signal i.e all CRs send at a logic 1 to the FC. The cooperative test using the AND rule can be formulated as follows:

$$H_1 : \sum_{k=1}^{K} \Delta_k = K$$
$$H_0: \text{Otherwise}$$

The **OR** decision rule decides a signal to be present if any of the CR users detects a signal. Hence, the cooperative test using the OR rule can be formulated as follows:

$$H_1 : \sum_{k=1}^{K} \Delta_k \geq 1$$
$$H_0: \text{Otherwise}$$

The third rule is the voting rule that decides on the signal presence if at least M of the K users have detected a signal with $1 \leq M \leq K$. The test is formulated as:

$$H_1 : \sum_{k=1}^{K} \Delta_k \geq M$$
$$H_0: \text{Otherwise}$$

A majority decision is a special case of the voting rule for M=K/2. It is the same as the AND and the OR rule which may also be considered to be special cases of the voting rule for M=K and M=1 respectively.

Quantized decision fusion: In this scheme, we try to realize a tradeoff between the overhead and the detection performance. Instead of one bit hard combining, where there is only one threshold dividing the whole range of the detected energy into two regions, a better detection performance can be obtained if we increase the number of thresholds to get more regions of observed energy.

In (J. Ma *et al*,2007), a two-bit hard combining scheme is proposed in order to divide the whole range of the detected energy into four regions as shown in Fig 7. The FC decides the presence of the signal of interest by using the following equation:

$$\sum_{i=0}^{3} w_i n_i \geq \lambda$$

where λ is the threshold which equals the weight of the upper region, n_i is the number of observed energies falling in region i and w_i is the weight value of region i with w_0= 0 w_1= 1, w_2= 2 and w_3= 4.

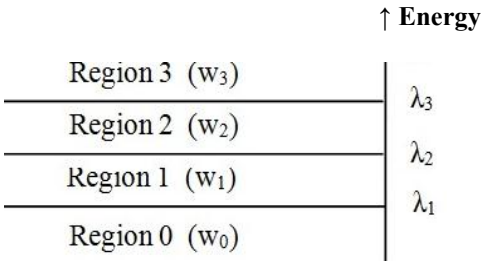

Fig 7: Two Bit Hard combination

Results presented in (P. Qihang *et al.2006)* show better performance than AND and OR-rules because the reliability of spectrum sensing at each secondary user is taken into account. The information fusion at the FC is made by considering the decisions of each CR and its credibility which is transmitted by cognitive radios along with their decisions. The credibility of CRs depends on the channel conditions and their respective distance from the licensed user. Optimum number of nodes for satisfying a probability of false alarm rate is investigated in (P. Pawełczak *et al*,2006*)*.

In addition to simple fusion rules, advanced fusion techniques can be devised to utilize the statistical knowledge for decision fusion. A linear-quadratic (LQ) fusion method is proposed in (J. Unnikrishnan *et al*, 2008) to consider the correlation between CR users in cooperative sensing. This method provides a suboptimal solution to the decision fusion problem because it uses the partial statistical knowledge, i.e the second-order statistics of the local decisions under H_1 and the fourth-order statistics under H_0. This method is based on the deflection criterion where the LQ detector compares a LQ function of the local decisions with a predetermined threshold thereby achieving better error probability with a higher value of deflection. The results have shown that this scheme outperforms the Counting Rule in correlated shadowing.

5. Security Concerns for CRNs

A cognitive radio network, especially if using cooperative spectrum sensing, can be susceptible to a variety of security challenges. These threats will include the traditional challenges of the wireless networks and threats specific to CRNs. We will concentrate on the threats which only CR networks face. These threats may be exogenous, greedy CR users or intruding malicious nodes. A brief overview of these attacks is as under:

Exogenous Attacks

In ad hoc CRNs the two classes of spectrum sensing attacks might be implemented by external adversary nodes. An exogenous attacker can mount PUAE or primary user emulation attack (also known as IE or Incumbent Emulation attack) or sensor jamming attacks on a CRN. In PUE attack the fusion center, FC, coordinates periods for spectrum sensing for the cooperating CRs and the results are fed back to the FC. Thus, the attacker can increase the local false-alarm

probability to skew the decision of the FC regarding the availability of a given band. In sensor jamming attack, exogenous attackers degrade the operation of a centralized CRN architecture, perhaps to the point of DoS (Denial of Service).This may be done by the following methods:

1. Common Control Channel Jamming
2. Receiver Jamming

Common Control Channel Jamming: Besides general wireless communication operations, the CCC in a CRN is utilized to carry out the spectrum sensing process. Therefore, disrupting the access to the CCC will severely affect a CRN. A jamming attack in resource access period can then have both short-term and long-term effects. If the jammed channel is the chosen channel to be sensed at a given period ***n*** by the CRN, the exogenous attacker will succeed in skewing the overall CRN sensing decision on the jammed channel to busy and thus deny the network from accessing that channel, thereby resulting in DoS. Furthermore, if this repeats a few times , the jammed channel will be less likely to be selected by the CRN in future also and hence affect the CRN operation in long term as well

Receiver Jamming: CR receivers, similar to other wireless technologies, require a minimum received SNR when trying to decode the signal from their corresponding transmitters. One of the oldest and most widely used attack strategies then is to degrade the received SNR to values below the required threshold by transmitting noise over the received channel (W. Xu *et al*, 2005; E. Altman *et al*, 2010). We refer to this attack technique as receiver jamming.

Intruding Attackers

CRNs are vulnerable to attacks from intruding adversary nodes which can penetrate into the network posing as legitimate nodes. These malicious nodes can affect the overall spectrum sensing decision of CRN by reporting misleading local sensing data. This type of CRN-specific security concern is known as the spectrum sensing data falsification (SSDF) (A. W. Min *et al*,2009*)*. In simplest type of SSDF attack, a channel is always reported busy or idle (S. Mishra *et al*,2006). More complex attackers though selectively provide false spectrum sensing reports to keep their attack strategy more difficult to identify (S. Sodagari *et al*,2010). Intruding nodes should however not be confused with greedy CRs, which might also falsify data with the aim of skewing the legitimate resource access competition within a CRN. The motivation for data falsification for greedy CRs and intruding nodes is different. For this reason Greedy CRs will be discussed separately.

Greedy CRs: A degree of competition in utilizing the available spectrum resources exists (L. Lifeng *et al*,2011)in ad hoc CRNs. Due to this competition some greedy CRs, which are authenticated and authorized members of the CRN, unlike intruding nodes, might deliberately falsify data in order to increase their chances of reserving the medium. As a result of this, greedy behavior of CR nodes reduces the total network capacity in spite of cooperative networking strategy (R. Etkin *et al* 2007; A. Attar *et al*, 2008). The possibility of untruthful behavior within the adopted MAC framework constitutes a security concern in ad hoc CRNs. As CRs are built upon software-defined radio (SDR) platform, a greedy CR can manipulate the backoff window in ALOHA style handshaking with random backoff mechanism so as to increase its probability of access to the spectrum.

6. Dealing with CRN Attacks

Different techniques evolved to deal with different types of CRN attacks. Some of these techniques are as listed under:

Exogenous attacks

Sensor Jamming: Cooperative spectrum sensing policies such as DSS, by providing a spatially distributed sampling of the sensed frequency channels inherently provides a safeguard mechanism against sensor jamming. There is a possibility that at any given time a number of sensing nodes may fall outside the coverage area of the sensor jammer and thus provide reliable sensing data. Hence it is necessary to identify the affected nodes and remove their sensing data from fusion rules or consensus algorithms. One potential solution, proposed in (A. W. Min *et al,2009;* A. W. Min *et al,2012*), is a shadow-fading correlation-based filter that allows sensing nodes within a cluster to detect abnormal sensing reports. This technique is mainly used to combat SSDF attacks, but can also be utilized to determine if certain areas within a cluster are facing jamming signals. These cluster-based cooperative sensing techniques can also improve the primary detection probability and make the network more resilient to sensor jamming.

Common Control Channel Jamming: Due to the point-to-point nature of communications in ad hoc CRNs, the network can adopt a non common control channel strategy. In this strategy nodes stay on each available channel for a certain time to identify any other node operating on a band in close proximity. Each node continues to jump between channels so as to develop a table of existing neighboring nodes and their operating channels. This non common control channel strategy is commonly used in mobile ad hoc networks MANETS. Using interference resilient waveforms, like spread-spectrum (SS) techniques and error detection and correction coding are some other solutions to combat control channel jamming.

Receiver Jamming: Due to their inherent frequency agility and the potential of PHY-layer reconfigurability, CRNs are more resilient receiver jamming attacks. A CRN still needs to conclusively determine if the poor performance of a receiving node is due to natural causes

like channel ailments and network congestion, or due to interference from a jamming attacker. The results in (W. Xu *et al,* 2005) verify that measuring signal strength and carrier sensing time can not conclusively determine the existence of a jammer.

It is proposed in (W. Xu *et al,* 2005) that there are two consistency checking parameters to detect an attacker. Anti-jamming techniques must be used to overcome the interfering effect upon detection of a receiver jammer. Spread spectrum techniques, such as Direct Sequence SS and frequency hopping SS, are some of the most widely used anti-jamming solutions for their superior performance in the presence of interference. Further, employing powerful error detection and correction codes can enhance the receiver performance in presence of jamming
signals.

Primary User Emulation Attack PUEA or Incumbent Emulation IE

An effective defense technique against PUAE attacks is based on verifying apriori known information regarding the primary transmitter such as the location of transmitters (e.g., TV broadcasting towers as the primary system is) (R. Chen *et al,2008*; R. Chen *et al,2008*).FCC has proposed to develop geolocation databases to enhance reliability of communications over TV white spaces, which can also serve as a verification source to identify real versus fake primary transmitters based on DRT or distance ratio test.

Intruding Node

Spectrum Sensing Data Falsification: Combating falsified sensing data in CRNs has received considerable research attention in recent past. Using shadow fading correlation-based filter in (A. W. Min *et al,2009*; A. W. Min *et al,2011*) is one way to cross check while, a trustworthiness score is proposed in (T. Qin *et al,2011*) where we develop a reputation weight for sensing nodes. It is proposed that we develop a trust-value indicator to detect malicious CRs through evaluating a suspicious level of nodes in (W. Wangz *et al,*2009). An outlier detection scheme based on prefiltering the sensing data is proposed in (P. Kaligineedi *et al,*2008).

Greedy CRs: Legitimate but the greedy CRs employ untruthful approaches, such as misreports, to place themselves at advantage compared with truthful CRs. A number of schemes can be employed to prevent such greedy misbehavior.

One way can be the monitoring of the behavior of CR nodes, by a centralized FC or the peer nodes, depending on the network architecture and provisioning punishment schemes to penalize detected greedy behavior. Another approach is misbehavior incentive reduction. e.g in (S. Sodagari *et al,*2010), a strategy to combat SSDF by greedy nodes is developed which is based on minimizing the difference in the utility of truthful and falsifying nodes in a DSS setting where incentive elimination for greedy nodes is employed. Utilizing fairness measures in scheduling, is another example where CR nodes in a centralized architecture can also reduce the motivation to report exaggerated CSI information.

In addition to solving problems inherent traditional wireless systems, such as in synchronization, precoding, beamforming, and transmit power control, work is being done in CRs to consider the effect of errors, intentionally induced by an attacker malicious or otherwise.

It is a challenge which is being tackled simultaneously at different levels by the researchers.

Conclusions

It has been established without a doubt that cognitive radio is the future of next generation wireless technologies. With large gains cooperative sensing is an effective technique to improve detection performance by exploring spatial diversity at the expense of cooperation overhead. In this paper, we discuss the cooperative sensing and especially the data fusion and decision fusion in detail. Also the various security threats that a CR network faces are also listed out. More work needs to be done in each area to make the CR networks of the future more robust with better sensing and fusion techniques and also newer and better, techniques to combat various security threats that a CRN is vulnerable to. When the CR networks become robust and secure the future of wireless communication will change forever for better.

References

S. Haykin (2005) Cognitive radio: Brain- empowered wireless communications, *IEEE Journal Selected Areas in Communications*,vol.23, no.2 pp.201-220.

Joseph Mitola III and Gerald Q. Maguire Jr. (1999), Cognitive Radio: Making software radios more personal,IEEE Personal Communications, 6 (4), pp. 13 18.

T Yucek and H Arslan (2009), A Survey of Spectrum Sensing Algorithms for Cognitive Radio Application, *IEEE Communications Surveys & Tutorials, **11**(1).*

I. F. Akyildiz, B. F. Lo and R. Balakrishnan (2011), Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey**,** *Physical Communication (Elsevier) Journal*, vol. 4, no. 1, pp. 40-62.

A.Ghasemi and E. Sousa (2005), Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments, *DySPANn* , pp 131–136.

I.F. Akyildiz, W.Y. Lee and K.R. Chowdhury (2009), CRAHNs: Cognitive radio ad hoc Networks, *Ad Hoc Networks* 7 (5) 810–836.

Longley-Rice Methodology for evaluating TV Coverage and Interference,(2004),OET Bulletin 69,Office of Engineering and Technology (OET),Federal Communications Commission

I.F. Akyildiz, W.-Y. Lee, M.C. Vuran and S Mohanty **(**2006),NeXt generation/ dynamic spectrum access/cognitive radio wireless networks: A survey, *Computer Networks 50* (13) 2127–2159.

D. Cabric, S. Mishra and R. Brodersen, (2004), Implementation issues in spectrum sensing for cognitive radios, *Proc. of Asilomar Conf.on Signals, Systems, and Computers*, vol. 1 , pp. 772–776.

S. Mishra, A. Sahai and R. Brodersen(2006), Cooperativ sensing among cognitive radios, *Proc. of IEEE ICC* vol. 4, pp. 1658–1663.

C. Sun, W. Zhang and K. Letaief (2007), Cooperativ spectrum sensing for cognitive radios under bandwidth constraints, *Proc. of IEEE WCNC* , pp. 1–5.

X. Zhou, G.Y. Li, D. Li, D. Wang and A.C.K. Soong (2010), Bandwidth efficient combination for cooperative spectrum sensing in cognitive radio networks , *Proc. of IEEE ICASSP*, pp. 3126–3129.

Z. Quan, S. Cui and A. Sayed (2008), Optimal linear cooperation for spectrum sensing in cognitive radio networks, *IEEE Journal of Selected Topics in Signal Processing*, 2 (1) 28–40.

W. Zhang and K. Letaief (2008), Cooperative spectrum sensing with transmit and relay diversity in cognitive radio networks, transaction letters, *IEEE Transactions on Wireless Communications* 7 (12) 4761–4766.

M. Di Renzo, L. Imbriglio, F. Graziosi and F. Santucci (2009), Distributed data fusion over correlated log-normal sensing and reporting channels: application to cognitive radio networks, *IEEE Transactions on Wireless Communications* 8 (12) 5813–5821.

K. Ben Letaief and Zhang (2009), Cooperative communications for cognitive radio networks, *Proceedings of the IEEE 97* (5) 878–893.

Z. Chair and P. K. Varshney (1986), Optimal data fusion in multiple sensor detection systems, *IEEE Trans. Aerosp. Electron. Syst.*, vol. 22, no. 1, pp. 98–101.

E. Visotsky, S. Kuffner and R. Peterson (2005), On collaborative detection of TV transmissions in support of dynamic spectrum sharing, *Proc.IEEE Int. Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Baltimore, Maryland, USA, pp. 338–345.

M. Gandetto and C. Regazzoni (2007) Spectrum sensing: A distributed approach for cognitive terminals, *IEEE J. Select. Areas Commun.*,vol. 25, no. 3, pp. 546–557.

F. Digham, M. Alouini and M. Simon (2003), On the energy detection of unknown signals over fading channels, in *Proc. IEEE Int. Conf.Commun.*, vol. 5, Seattle, Washington, USA, pp. 3575–3579.

V. I. Kostylev (2002), Energy detection of a signal with random amplitude, *Proc. IEEE ICC*, pages 1606–1610.

Zhi Quan, Shuguang Cui, H. Vincent Poor and Ali H. Sayed (2008), Collaborative wideband sensing for cognitive radios, *IEEE Signa Processing Magazine*, Vol. 25, No. 6, pp. 63– 70.

J. Ma and Y. Li (2007), Soft combination and detection for cooperative spectrum sensing in cognitive radio networks, *Proc. IEEE Global Telecomm. Conf.*, pp. 3139–3143.

Zhengquan Li, Peng Shi, Wanpei Chen and Yan Yan (2011), Square Law Combining Double threshold Energy Detection in Nakagam Channel, *International Journal of Digital Content Technology and its Application*, volume5,Number 12.

M. K. Simon and M.-S. Alouini (2004),Digit communication over fading channels, Joh Wiley & Sons, Inc., 2 ed.

Z. Quan, S. Cui and A. Sayed (2008), Optima linear cooperation for spectrum sensing cognitive radio networks, *IEEE Journal of Selected topics in Signal Processing 2* (1) 28–40

P. Qihang, Z. Kun, W. Jun and L. Shaoqi (2006), A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context, *Proc. IEEE Int. Symposium on Personal, Indoor and Mobile Radio Commun.*, pp. 1–5.

P. Pawełczak, G. J. Janssen and R. V. Prasad (2006), Performance measures of dynamic spectrum access networks, *Proc. IEEE Global Telecomm. Conf. (Globecom)*, San Francisco, California, USA.

J. Unnikrishnan and V.V. Veeravalli (2008 Cooperative sensing for primary detection in cognitive radio, *IEEE Journal of Selected Topics in Signal Processing* 2 (1) 18–27.

A.Attar, H.Tang, A.V.Vasilakos, F.R.Yu an V.C.M.Leung, (2012), A survey of security challenges in cognitive radio networks: Solutions and future research directions, *Proceedings of the IEEE, Vol. 100, No. 12*, pp. 3172-3186.

W. Xu, W. Trappe, Y. Zhang and T. Wood (2005), The feasibility of launching and Detecting jamming attacks in wireless Networks, *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw.Comput.*,Urbana, IL,pp.46– 57.

E. Altman, K. Avrachenkov and A. Garnaev, B, (2010), Jamming in wireless networks under uncertaint *Mobile Netw. Appl*., vol. 16, no. 2, pp. 246–254 .

A. W. Min, K. G. Shin and X. Hu (2009) Attack- tolerant distributed sensing for dynamic spectrum access networks, Proc. 17th IEEE Int. Conf. Netw. Protocols, pp 294–303.

S. Sodagari, A. Attar, V. Leung and S. B (2010), Denial of service attacks in cognitive radio networks through channel eviction triggering, *Proc. IEEE Global Telecommun. Conf., Miami, FL*, DOI: 10.1109/GLOCOM. 5683177.

L. Lifeng, H. El Gamal, J. Hai and H. V.(2011), Cognitive medium access:explorati exploitation, and competition, *IEEE Tra Mobile Comput.*, vol. 10, no. 2, pp. 239–253

R. Etkin, A. Parekh and D. Tse (2007),Spect sharing for unlicensed bands, *IEEE J. Areas Commun.*, vol. 25, no. 3, pp. 517–528.

A. Attar, M. R. Nakahi, and A. H.Aghvami (2008), Cognitive radio game for second spectrum access problem, *IEE Trans.Wireless Commun*., vol. 8, no. 4, pp. 2121–2131..

A. W. Min, K. G. Shin and X. Hu (2009), Attack-tolerant distributed sensing dynamic spectrum access networks, *P 17th IEEE Int. Conf. Netw. Protocols, Princeton, NJ*, pp. 294–303.

A. W.Min, K. G. Shin and X. Hu (2011), Secure cooperative sensing in IEEE 802.22 WRA using shadow fading correlation ,*IEEE Trans. Mobile Comput.*, vol. 10, no. 10, pp. 1434–1447.

W. Xu, W. Trappe, Y. Zhang and T. Wood (2005),The feasibility of launching and detecting jamming attacks in wireless networks, in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., Urbana, IL,* pp 46–57.

R. Chen, J.-M. Park and J. H. Reed (2008) Defense against primary user emulate attacks in cognitive radio networks, *IEEE J. Sel. Areas Commun.*,vol. 26, no.1, pp. 25–37.

R. Chen, J.-M. Park, Y. T. Hou and J. H. Re (2008), Toward secure distributed spectrum sensing in cognitive radio networks, *IEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55.

T. Qin, H. Yu, C. Leung, Z. Shen and C.Mia (2009), Towards a trust aware cognitive radio architecture, *ACM Mobile Comput. Commun.Rev*., vol. 13, no. 2, pp. 86–95.

W. Wangz, H. Liy, Y. Sunz and Z. Han (2009) Attack-proof collaborative spectrum sensing in cognitive radio networks, *Proc. Conf. Inf. Sci. Syst., Baltimore, MD*,pp. 130–134.

P. Kaligineedi, M. Khabbazian and V Bharrgava (2008),Secure cooperative sensing techniques for cognitive radio systems, *IEEE Int. Conf. Commun.*, pp. 3406–3410.

Teguig, Scheers and V.Le.Nir (2012), Data Fusion Schemes for cooperative Spectrum Sensing in Cognitive Radio Networks,*Military Commun. and information sys Conf. (MCC),* pp.1-7.

R. Viswanathan and P. Varshney (1997), Distributed detection with multiple sensors: part I— fundamentals, *Proceedings of th IEEE 85 (1)* pp.54–63.

P.K. Varshney (1997), Distributed Detection and Data Fusion, Springer-Verlag, New York.