Spectrum Sensing and Security Challenges and Solutions: Contemporary Affirmation of the Recent Literature

Shribala Nagul[1], Dr. Srihari[2] and Dr. B C Jinaga[3]

[1] Bhoj Reddy Engineering College for Women

Received: 10 December 2013 Accepted: 31 December 2013 Published: 15 January 2014

Abstract

Cognitive radio (CR) has been recently proposed as a promising technology to improve spectrum utilization by enabling secondary access to unused licensed bands. A prerequisite to this secondary access is having no interference to the primary system. This requirement makes spectrum sensing a key function in cognitive radio systems. Among common spectrum sensing techniques, energy detection is an engaging method due to its simplicity and efficiency. However, the major disadvantage of energy detection is the hidden node problem, in which the sensing node cannot distinguish between an idle and a deeply faded or shadowed band. Cooperative spectrum sensing (CSS) which uses a distributed detection model has been considered to overcome that problem. On other dimension of this cooperative spectrum sensing, this is vulnerable to sensing data falsification attacks due to the distributed nature of cooperative spectrum sensing. As the goal of a sensing data falsification attack is to cause an incorrect decision on the presence/absence of a PU signal, malicious or compromised SUs may intentionally distort the measured RSSs and share them with other SUs. Then, the effect of erroneous sensing results propagates to the entire CRN. This type of attacks can be easily launched since the openness of programmable software defined radio (SDR) devices makes it easy for (malicious or compromised) SUs to access low layer protocol stacks, such as PHY and MAC. However, detecting such attacks is challenging due to the lack of coordination between PUs and SUs, and unpredictability in wireless channel signal propagation, thus calling for efficient mechanisms to protect CRNs. Here in this paper we attempt to perform contemporary affirmation of the recent literature of benchmarking strategies that enable the trusted and secure cooperative spectrum sensing among Cognitive Radios.

Index terms— cognitive radio network, secure spectrum sensing, mobility and trust, cognitive radio, symmetric cryptographic key generation, LT code.

1 Introduction

ireless technology is increasing swiftly, and the view of pervading wireless computing and communications offers the potential of many interpersonal and solitary pros. While individual gadgets in particular mobile phones, smart phones and notebook computers be given a lot of consideration, the effect of wireless engineering is much more comprehensive, e.g., implies sensor networks for protection applications and home automation, smart grid control, body sensor devices and embedded wireless devices, and entertainment systems. This increase of wireless solutions brings about an everincreasing demand for more radio spectrum. Conversely, most quickly accessible spectrum bands being given, despite the fact that various investigations have actually indicated that these bands are substantially underneath in utilization. These factors to consider have encouraged the radio technologies that can level to reach foreseeable future requirements equally in terms of spectrum effectiveness and application functionality.

Cognitive radios come with the promise of being a troublesome engineering advancement that will make it possible for the future telecommunication world. Cognitive radios are thoroughly automated cordless devices that can perceive their settings and dynamically adjust their transmitting waveform, channel access method, spectrum use, and networking protocols as needed for good networking and device performance. We foresee that cognitive radio engineering will eventually come up from initial phase research studies and to become a general-purpose automated radio that will suffice as a widespread platform for wireless system advancement, far similar to microprocessors, which have served a similar role for computation. There is conversely a big gap among having an adaptable cognitive radio, reliable building block, and the extensive deployment of cognitive radio networks that dynamically maximize spectrum usage.

2 II.

3 Contemporary Affirmation of the

Literature of Secure Spectrum Sensing in [2], study impact of mobility on collaborative spectrum sensing. The authors show that because of mobility, the secondary user sensing results get uncorrelated faster thus giving better performance compared to spectrum sensing performed by static secondary users but does not consider the presence of malicious users. To identify the malicious users in the CRN, the evaluation of trust for each secondary user under collaborative spectrum sensing has been addressed using different techniques in the literature. In the solution proposed by authors in [5], secondary users in close proximity are grouped into clusters and the system detects abnormal reports using shadow-fading correlation filters. The authors in [4] evaluate the secondary users trust, comparing deviation suffered by each secondary user's sensing measurement from the average measurement reported at the fusion center. The Bayesian rule is applied in [6] to compute the a posteriori probability of being an attacker for each secondary user. When the posteriori probability of a certain secondary user exceeds the suspicious level threshold, it is claimed to be an attacker and is removed from the collaboration. For multiple attackers, the large number of combinations of attackers and honest users is removed by using an onion-peeling based approximation to reduce computational complexity. Abnormality detection algorithm based on proximity, which is widely used in the field of data mining has been introduced in [3], to solve the problem of malicious users in the system using history reports of each secondary user. The proposed architecture in [7], needs to collect spectrum sensing data from multiple sources or equipment on consumer premises. This process is known as crowd sourcing. The authors consider the area of interest is divided in cells and the credibility of these devices are kept in check by corroboration and merging among neighboring cells. The corroboration in a hierarchical structure is used to identify cells with significant number of malicious nodes. To the best of our knowledge, none of the existing work studied malicious and primary user detection for mobile CRNs. Our proposed solutions are different from all the existing solutions that we separate the location reliability from the user trust, thus achieve better performance on malicious user detection.

The rapid growth in wireless communications has contributed to a huge demand on the deployment of new wireless services in both the licensed and unlicensed frequency spectrum. However, recent studies show that the fixed spectrum assignment policy enforced today results in poor spectrum utilization. To address this problem, cognitive radio (CR) [8,9] has emerged as a promising technology to enable the access of the intermittent periods of unoccupied frequency bands, called white space or spectrum holes, and thereby increase the spectral efficiency. The fundamental task of each CR user in CR networks, in the most primitive sense, is to detect the licensed users, also known as primary users (PUs), if they are present and identify the available spectrum if they are absent. This is usually achieved by sensing the RF environment, a process called spectrum sensing [8][9][10][11]. The objectives of spectrum sensing are twofold: first, CR users should not cause harmful interference to PUs by either switching to an available band or limiting its interference with PUs at an acceptable level and, second, CR users should efficiently identify and exploit the spectrum holes for required throughput and qualityof service (QoS). Thus, the detection performance in spectrum sensing is crucial to the performance of both primary and CR networks. The detection performance can be primarily determined on the basis of two metrics: probability of false alarm, which denotes the probability of a CR user declaring that a PU is present when the spectrum is actually free, and probability of detection, which denotes the probability of a CR user declaring that a PU is present when the spectrum is indeed occupied by the PU.

The idea of using Beta Reputation System as reputation evaluation system has been proposed in **??**12] in which a node's confidence in its spectrum sensing report is used as a weight during calculation of spectrum decisions. This work assumes that the PU's transmission range is large enough to be received by all nodes in the CRN including the SU base station (SUBS), the controlling entity of the CRN. It also assumes that the PU can communicate with SUBS, wherein a PU may complain to the SUBS regarding any interference caused by CRN operation. Since this work assumes that the PU cannot sell its unused spectrum bands, therefore there is no incentive for it to communicate with the CRN. This communication may cost a PU, additional hardware and/or system complexity, just to inform the CRN regarding interference caused to its communications. Furthermore, need for any changes to the incumbent PU. This work also does not deal with any mobility by SUs or PUs.

A collaborative spectrum sensing scheme is presented in [13] which introduces Location Reliability and

Malicious intent as trust parameters. The authors employ the Dempster-Shafer theory of evidence to evaluate trustworthiness of reporting secondary user nodes. The proposed scheme assigns trust values to different cells in the network which may receive abnormal levels of PU's signal due to the effects of multi-path, signal fading and other factors in the radio environment. Equal emphasis is given to the spectrum sensing reports from SUs using Equal Gain Combining while using trust values of the cells from where these reports were received as weights for data aggregation. This approach also assumes that the PU's communication range is large enough to be received by the entire CRN and uses the spectrum sensing reports of all CRN nodes to reach the final spectrum decision.

Authors in [4] and [14] assume that the transmission range of PU is large enough to be received in the entire CRN. [4] Proposes pre-filtering to remove extreme spectrum sensing reports and a simple average combining scheme to calculate spectrum sensing decisions while considering all reports that pass the prefiltering phase. [14]Characterizes the spectrum sensing problem as an M-ary hypotheses testing problem and considers a cluster-based CRN where cluster heads receive and process raw spectrum sensing data before forwarding to the fusion center. Since PU's transmission range is assumed to be large enough to be received by every node in the network, both approaches cannot be adopted for a CRN in which a PU has smaller transmission range than the size of CRN.

Muhammad Faisal Amjadet al [81] proposed a novel reputation aware collaborative spectrum sensing framework based on spatio-spectral anomaly detection. Their proposed system is well suited for situations where the PU's communication range is limited within a subregion of the CRN. Simulations of their system shown that it is robust against SSDF attacks and can detect malicious behavior up to 99.3 percent of the time when malicious node density is within a reasonable range and is still very effective when the number malicious nodes is even greater. Their proposed system is also flexible enough to be used where PU's communication range spans the entire CRN.

4 b) Secure Cooperative Spectrum Sensing in Cognitive

Radio Networks CR related research has received great attention recently. Because its dynamic spectrum access is fundamentally different from conventional wireless systems, there is a need to design different components in the protocol stack. The physical layer requires most fundamental change. A major research problem is how to correctly detect the existence of primary users and spectrum opportunities. In [15], Challapaliet. al proposes to use Hough Transform and autocorrelation function to detect spectrum opportunities. A more direct approach was presented in [16] to observe primary user's signal-to-noise ratio (SNR) and entropy for seeking spectrum opportunities. A spectrum opportunity is recognized only when a spectrum has both low SNR and low entropy. According to [15], these schemes belong to collocated sensing architectures, since a single secondary user device carries on the spectrum sensing task and makes an independent decision to access a spectrum. However, due to the hidden-terminal problem, such a scheme may show poor performance in terms of miss detection and false alarm probabilities. To address this problem, techniques for cooperative spectrum sensing was investigated. In the authors utilize the fact that noise is independent at different users while signals are correlated, so adding up the received signals at two secondary users can increase SNR and improve detection accuracy. A similar approach is used in to increase detection sensitivity. The authors of [20,22] employ sensors for distributed spectrum sensing. In [20], some sensors are placed close to primary receivers to detect their local oscillator leakage power, and then these sensors relay the detection information to secondary users. In [15], an independent sensor network is proposed to be deployed specially for spectrum sensing. All secondary users query the sensor network to learn the information about spectrum opportunities. In the link layer, CR related research mainly investigates new media access control (MAC) protocols to adapt to the dynamic change of spectrum opportunities. These protocols are more or less derived from conventional wireless MAC protocols. For example, DC-MAC [21] is a slotted MAC protocol similar to ALOHA but with an enhanced mechanism to optimize per-slot throughput; DOSS protocol was derived from MAC protocols based on busy tone; and CR MAC protocol [17] generalizes 802.11 into supporting multiple channels. There is less research on the network layer or layers above since the lower layers are still not welldefined for CR networks. However, there has been research that takes cross-layer approaches to optimize network or above layer objectives by defining MAC or physical layer behaviors [19,21]. Although security is an important aspect of spectrum sensing, to the best of our knowledge, there is virtually no previous work that addresses this issue. In the authors discuss the impact of malicious users on the required sensing sensitivity of individual terminals when cooperative spectrum sensing is performed. However, methods to ensure the robustness of spectrum sensing were not discussed.

There has been a growing interest in attackresilient collaborative spectrum sensing in CRNs. Liu et al. [22] exploited the problem of detecting unauthorized

5 Global Journal of Computer Science and Technology

Volume XIV Issue V Version I usage of a primary licensed spectrum. In this work, the path-loss effect is studied to detect anomalous spectrum usage, and a machine-learning technique is proposed to solve the general case. Chen et al. [23] focused on a passive approach with robust signal processing, and investigated robustness of various data-fusion techniques against sensing-targeted attacks. Kaligineedi et al. [4] presented outlier detection schemes to identify abnormal sensing reports. Min et al. [24]proposed a mechanisms for detecting and filtering out abnormal sensing reports by exploiting shadowfading correlation in received primary signal strengths among nearby SUs. Fatemiehetal. [7]used outlier measurements inside each SU cell and collaboration among neighboring cells to identify cells with a significant number of malicious nodes. Li et al. in [24]detected possible abnormalities according to SU sensing report histories. Our work is different from existing approaches in three aspects. First, we consider cooperation among attackers, so the attacks are much more challenging to prevent. Second, unlike the previous work which focused on sensing data falsification attacks, we also consider the case where the attackers violate the fusion center's decision regarding spectrum access. Finally, our proposed attack-prevention mechanisms can easily prevent attacks without differentiating attackers from honest SUs.

The problem of ensuring robustness in distributed sensing has been studied in [23], [4], and [27]. Chen et al. [23] proposed a robust data-fusion scheme that dynamically adjusts the reputation of sensors based on the majority rule. Similarly, in the IEEE 802.22 standard draft, a voting rule [27] has been proposed for secure decision fusion. Kaligineedi et al. [4] presented a profiteering scheme based on a simple outlier method that filters out extremely low or high sensor reports. However, their method may not suitable fora very low SNR environment such as 802.22 WRANs wherea final data-fusion decision is very sensitive to small deviations in RSSs. The defense against Primary User Emulation Attack (PUEA) has also been studied in [25]and [26]. Chen et al. [25] proposed an RSS-based location verification scheme to detect a fake primary transmitter. This scheme, however, requires the deployment of a dense sensor network for estimating the location of a signal source, and thus, incurs high system overhead. Anand et al. [26] analyzed the feasibility of PUEA and presented a lower-bound on the probability of a successful PUEA. However, they did not address the impact of PUEA on the performance of cooperative sensing. The problem of enforcing/enticing secondary users to observe spectrum etiquette has also been studied. Woyachet al. [28] studied how to entice secondary users to observe spectrum etiquette by giving them incentives. In a similar context, Liu et al. [22] studied the problem of detecting unauthorized use of a licensed spectrum. They exploited the path-loss effect as a main criterion for detecting anomalous spectrum usage and presented a machine-learning approach for more general cases. In contrast, we focus on intelligent filtering of suspicious sensor reports. In a broader context, our paper is related to work on secure data aggregation [29], [30], [31] and insider attack detection [32] in wireless sensor networks. However, the problem we consider differs in that it focuses on an important, realistic case where attackers manipulate sensor reports to mislead the fusion center in making a final decision on detection of a primary signal.

In order to entice SUs to follow the protocol, i.e., reporting the sensing results honestly, researchers used game-theoretic approaches to analyze SUs' behavior. Duan et al. [34] proposed attack prevention mechanisms with direct and indirect punishments. Assuming that SUs care for their rewards, their scheme prevents SUs from reporting falsified sensing data by setting appropriate reward and punishment functions. Woyach et al. [28] developed a model for the incentives associated with attacks and for the tradeoffs between the different elements of an enforcement structure.

To detect discrepancies among sensing data and ensure robust decisions in cooperative spectrum sensing, researchers have studied robust data-fusion in CRNs. Kaligineedi et al. [4] introduced a trust factor which gives a measure of reliability of each SU. By applying an outlier detection method, their data-fusion scheme assigns a lower trust factor to a SU whose sensing report is extremely high or low, reducing its effect on the sensing decision. Chen et al. [23] presented a weighted sequential probability ratio test which introduces a reputation-based mechanism to the sequential probability ratio test (SPRT). By increasing the reputation of a SU whose sensing report is consistent with the majority at each step, their scheme dynamically adjusts the weight of each SU so that a SU with higher reputation can have more influence on the sensing decision. Min et al. [33] proposed a correlation filter for the detection of abnormal sensing reports by exploiting the shadow fading correlation in RSSs.

Assuming that RSSs at nearby SUs are correlated, they proposed a clustering method and data-fusion rules based on the correlation analysis of sensing reports.

These defense schemes, however, have their own limitations in that their assumptions may not hold. Game-theoretic attack prevention assumes that SUs try to maximize their utilities by following the protocol. However, considering that attackers outside of a network can compromise inside of the network. These schemes may not work well if these attackers do not care about compromised SUs' utilities. Robust datafusion schemes compare sensing data among SUs assuming that the numbers of honest SUs are much larger than that of malicious/compromised SUs which mount sensing data falsification attacks. Obviously,

6 Global Journal of Computer Science and Technology

Volume XIV Issue V Version I 36(D D D D)

Year 2014 robust fusion schemes may not be suitable for detecting attacks when the number of honest SUs becomes small. Noting that this number can easily be reversed in a network of a small number of SUs, CRNs are required to be capable of detecting attacks even when the number of honest SUs is small.

Cooperative spectrum sensing has received considerable attention as a viable means to enhance the detection performance by exploiting spatial diversity in received signal strengths. However, this is vulnerable to sensing data falsification attacks due to the distributed nature of cooperative spectrum sensing. To overcome this problem, we introduce a primary user emulation test (PUET), under which a trustful central entity (e.g., a cellular base station) transmits a test signal while other users are sensing the spectrum. The core of PUET is to correlate the reported sensing data with the transmission power of the test signal. Since this test signal is, in reality, interference to the sensing of a primary signal, sensors cannot distinguish the test signal from the primary signal. Considering this characteristic of sensors, PUET detects attacks by evaluating the consistency of channel parameters, which are not known to sensors. By recognizing this defense mechanism, PUET checks the validity of reports from each sensor separately. The efficacy of PUET is validated via experimentation on a test bed deployed in an indoor environment. Our measurement study shows that PUET achieves over 95% detection rate while keeping the false alarm rate under 5%.

Seunghyun Choi et al [82] proposed the design of reliable distributed sensing for opportunistic spectrum use is a major research challenge in DSA networks. To meet this challenge, they proposed PUET that detects the falsification of sensing results. The key idea behind PUET is that CPEs can acquire only RSSs, not the information of the signal source. To realize this idea, the BS transmits a test signal when CPEs sense the channel. Since CPEs cannot distinguish a test signal from a PU signal, the BS can detect sensing data falsification attacks by checking if the reported sensing data reflects the test signals it transmitted. In order to check the validity of sensing reports, the BS tests three consecutive sensing reports in a testing window. By checking the consistency of estimation of the received primary signal strength, the BS determines if there exist nonzero attack strengths in the sensing reports. They have evaluated the performance of attack detection with an indoor USRP2-based test bed. By conducting experiments on the test bed, we have confirmed that PUET detects attacks with both random and ON/OFF attack strengths. They have also found that PUET correctly detects PU signals even when more than a half of reports are faulty.

noise channel was first addressed by Urkowitz [37]. In his proposal, the receiver consisted of an energy detector which measures the energy in the received waveform over an observation time window. This energy-detection problem has been revisited recently by Kostylev in **??**36] for signals operating over a variety of fading channels. Our contribution in this letter is twofold. First, we present an alternative analytical approach to the one presented in[36] and obtain closed-form expressions for the probability of detection over Rayleigh and Nakagami fading channels. Second, and more importantly, we quantify the improvement in detection capability (specially for relatively low-power applications) when low-complexity diversity schemes such as square-law combining (SLC) and square-law selection (SLS)are implemented. While diversity analysis is carried out for independent Rayleigh channels for the SLS scheme, both independent and correlated cases are considered for the SL Cone. For more details, the reader is referred to [35].

The underutilization of the radio spectrum as revealed by extensive measurements of actual spectrum usage [38] has stimulated exciting activities in the engineering, economics, and regulation communities in searching for better spectrum management policies. The diversity of the envisioned spectrum reform ideas is manifested in the number of technical terms coined so far: dynamic spectrum access's. Dynamic spectrum allocation, spectrum property rights vs. spectrum commons, opportunistic spectrum access vs. spectrum pooling, spectrum underlay vs. spectrum overlay. Often, the broad term "cognitive radio" is used as a synonym for dynamic spectrum access. As an initial attempt at unifying the terminology and documenting recent developments, we provide a taxonomy of dynamic spectrum access and an overview of the technical challenges and advances in this emerging research area.

Radio spectrum is a valuable commodity, and a unique natural resource shared by various types of wireless services. Unlike other natural resources, it can be repeatedly re-used, provided certain technical conditions are met. In practice radio spectrum can accommodate a limited number of simultaneous users. Therefore, radio spectrum requires careful planning and management to maximise its value for all users. Currently, spectrum regulatory framework is based on static spectrum allocation and assignment policy. Radio spectrum is globally allocated to the radio services on the primary or secondary basis. This is reflected in the Radio Regulations published by the International Telecommunication Union (ITU) **??**39], which contains definitions of these services and a table defining their allocations for each of three ITU geographic world The PROBLEM of detecting an unknown deterministic signal over a flat band limited Gaussian regions. On the European level, radio spectrum is governed in the European Union by the Radio Spectrum Policy Group (RSPG) and Radio Spectrum Committee (RSC) and by European Conference of Postal and Telecommunications Administrations (CEPT). Additionally, national regulatory agencies define national allocation table and assign radio spectrum to licence holders on a long term for large geographical regions on exclusive basis. Generally, user can use radio spectrum only after obtaining individual license issued by national regulatory agency. In technical point of view, this approach helps in system design since it is easier to make a system that operates in a dedicated band than a system that can use many different bands over a large frequency range. In addition, spectrum licensing offers an effective way to guarantee adequate quality of service and to prevent interference, but it unfortunately leads to highly inefficient use of radio spectrum resource. Analyzing Article 5 of Radio Regulations [39], and national allocation tables it can be concluded that usage of radio spectrum bands is already determined. Furthermore, in national spectrum assignment databases almost all frequency bands of commercial or public interest are already licensed. Current predictions of further growth of demand for wireless communication services show substantial increase in demand of radio spectrum. All of this circumstances support raising serious concerns about future radio spectrum shortages. Nevertheless, related radio spectrum observation surveys have proved that most of the allocated spectrum is underutilized [40][41] **??**42][43][44][45][46]. FCC's measurements in Atlanta, New Orleans, and San Diego in 2002 revealed that there are large variations in the intensity of spectrum use below 1 GHz [40,41].

By observing two non-adjacent 7 MHz spectrum bands with a sliding 30 second window, the measurements showed that a fraction of 55-95 % of the observed frequencies were idle during the observation period on one band while on the other band the frequencies were almost fully idle. Shared Spectrum Company conducted spectrum occupancy measurements on the bands between 30 MHz and 3 GHz at six locations in the USA ??42]. The average occupancy over the locations was found to be only 5.2 % with the maximum occupancy 13.1 % in New York City and minimum occupancy 1 % in a rural area. Similar spectrum measurements conducted in Europe [43][44][45][46] (Germany, Spain, Netherlands, Ireland, France, Czech Republic) shows higher spectrum occupancy comparing to USA, but still rather low (e.g. 32% for the band 20-3000 MHz in Aachen area, Germany). Generally it can be concluded that spectrum occupancy is moderate below 1 GHz and very low above 1 GHz.

Radio spectrum is as carcere source. The regulatory body Federal Communication Commission (FCC) is responsible for radio spectrum resources and regulation of radio emissions. The FCC assigns spectrum to licensed holders, primary users(PU)on a long term basis for large geographic alregio However, FCC found that most radio frequency spectrum was underutilized or in efficiently utilized. Therefore, now they have proposed then otion of secondary utilization where the users who have no spectrum licenses, these condary users (SU)are allowed touse temporarily unused licensed spectrum. Cognitive radio technology has brought are volutionary change in communication par adig man disreceivinga growing attention in recenty ears [47]. This technology can provide faster and more reliable wireless services by utilizing the existing spectrum band more efficiently and without interference to primary users. The cognitive radio network users need to be aware of dynamic environment and adaptively adjust their transmission or reception parameters based on interactions with the environment and other users in the network to execute its task efficiently without interfering with licensed users or other cognitive radios. Since, cognitive radio is a secondary user; it has to vacate the band immediately as soon as there is arrival of primary user. Therefore, it is indeed very important for cognitive radio that transmissions hould be achieved with less bandwidth requirement and that correct data decoding should be possible at receiver side without the need of ACK (acknowledge) signal and Automatic Repeat Request (ARQ). To overcome this problem, a new class of erasure correcting codes known as fountain codes (also known as rate less erasure codes) is introduced and is under consideration to be used for transmission over cognitive radio network. The fountain code acts as a channel code to combat the effects of loss against PU interference and other channel conditions and helps receiver to decode complete data accurately. The fountain code produce limit less number of encoded symbols from given set of source symbols such that original source symbols can be recovered from any subset of encoded symbols of size equal toors lightly larger than number of source symbols. There are two classes off ounta in codes: Lu by Trans form(LT) codes and Raptor codes. Although Raptor codes are the most efficient codes, a new class of fountain codes, Raptor Q code sh as been introduced recently which seems to be more promising than its previous version Raptor code with increase do ding efficiency and improved reception over head and with performance almost like ideal performance of fountain code.

With explosive increase in demand for additional frequency spectrum, cognitive radios (CRs) were offered to support existing and new services. CR scenarios were proposed to improve spectrum efficiency and to solve the normally occurring spectrum scarcity. CR is also highly agile wireless platform, so it is capable of autonomously choosing operating parameters based on both frequency spectrum and network conditions. CRs promise an enhanced utilization of the limited spectral resources. In CR scenarios, secondary users (SUs) and primary users (PUs) coexist simultaneously [47], [48][49][50][51].

The detection of PUs can be accomplished by opportunistic spectrum sharing [50,52]. In opportunistic spectrum sharing, the PU usage is automatically monitored by SUs based on CR scenario. In the CR scenarios, no changes have to be made to legacy systems as the PU is unaware of the secondary usage of its spectrum. Since the arrival of a PU acts like an erasure on the SU link, it causes the SU to lose all the packets that are being transmitted over the channel which was under that particular PU's carrier. In order to overcome this problem caused by PU arrival on the SU link, some techniques have been proposed in [53]. In fact, any method to employ some sort of feedback procedures is not practical over CR network, indeed, once the channel has been captured by a PU, the retransmission request has to be placed on a different channel, which may not be available or reliable. So in order to avoid the need for a feedback channel, erasurecorrecting codes are suggested [54]. Hence, the packets that are lost due to PU interference are now considered as erasures. The erasure-correcting codes used in our model are digital Fountain codes.

The concept of digital Fountain codes was first introduced by Byers et al. [55,56] in 1998 for information distribution. Fountain codes are a class of erasure codes with the property that a potentially limitless sequence of encoding symbols can be generated from a given set of source symbols. The original source symbols can ideally be recovered by the decoder from any subset of the received coded symbols of size equal to or only slightly larger than the number of source symbols. The term fountain or rate less refers to the fact that these codes do not exhibit a fixed code rate. In [57] a solution to further enhance the performance of cognitive radio networks is proposed.

LT complexity of the encoding and decoding is very low [54]. Some networks, such as cognitive radio networks, do not have a feedback channel. Applications on these networks still require reliability. The SU link of cognitive radio can be modeled as a two states channel. One state is influenced by channel fading and noise but the other is like erasure channel. Thus, erasure code is a good choice for cognitive radio [58]. On the other hand, in cognitive radio network, it is normal to assume that there are no network attackers and the participants involved in the protocols are honest. But attackers always try to corrupt data anyway. As a result, a secure code is essential that can save time and cost.

As mentioned the successful deployment of CR networks and the realization of their benefits depend on the placement of essential security mechanisms in sufficiently robust form to resist misuse of the systems. Ensuring the trustworthiness of the spectrum sensing process is important in the CR networks, since spectrum sensing directly affects spectrum management and incumbent coexistence [59][60][61][62][63].

Hosseiniet al., [83] presented a secondary link channel model and then secure LT code is proposed to supply security and reliability simultaneously. In the proposed block, a code matrix is used for generation of cryptographic key. Cryptographic key is not sent over the channel; as a result, the frequency spectrum is saved. Also coder information is used to generate cryptographic key.

The importance of security in a cognitive radio network must highly be recognized. Since CR scenario permits attackers to easy and unauthorized access. First of all, secondary link channel model is proposed and a combinational block is proposed for a secure LT code, as well as providing security and error correction capability simultaneously. In SLC, a generator matrix is used to generate a random cryptographic key. SLC supply security without transmitting the key in a symmetric cryptography in a secure channel, as a result, the increase in spectrum efficiency becomes apparent. This implies saving time and costs. Besides, the key does not appear on channel, consequently, the attackers have to consider all possible key combinations. This block is useful in all communication systems that have no feedback channel.

7 d) Trusted Collaborative Spectrum Sensing

In cognitive radio networks (CRNs), spectrum sensing must meet the strict ”ability to detect” requirements set by the FCC to protect primary users’ communications from excessive interference caused by secondary CR devices. To meet these requirements, cooperative sensing [58] and sensing Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific scheduling [64,67] have been studied as efficient means to improve the sensing performance by exploiting spatio-temporal diversity in received signal strengths (RSSs). In [67], we proposed a sensing framework that minimizes the sensing-time while meeting the detection requirements by jointly optimizing sensor selection and sensing scheduling. An interesting observation made there is that when sensors are stationary as in 802.22 WRANs, the measured RSSs at each sensor are pseudo timeinvariant, depending on their geographic allocation, thus limiting the performance gain from sensing scheduling. Mobility is one of the most important factors in wireless systems because it affects numerous network characteristics, such as network capacity , connectivity, coverage [65], routing [66], etc. It is also an inherent feature to support various types of wireless services in CRNs. While the 802.22 Working Group considered only stationary sensors (i.e., CPEs) in the initial standard draft, recently, they adopted an amendment for the operation of portable devices. Despite its importance, however, mobility is still largely unexplored in the context of dynamic spectrum access. Allowing sensor mobility in CRNs will introduce numerous challenges, making it necessary to revisit current system design and protocols, such as mechanisms for spectrum sensing, interference management and routing. As a first step to understand the impact of mobility in CRNs, we study the performance of spectrum sensing with mobile sensors via a theoretical study. In particular, we show that, when sensing is scheduled multiple times, sensor mobility can yield a significant performance gain by exploiting spatiotemporal diversity in received primary signal strengths. This is in sharp contrast to the case of stationary sensors where the benefit to be gained from scheduling sensing is marginal. Our theoretical analysis indicates that the contribution of sensing scheduling to the performance improvement increases as the speed of mobile sensor increases, raises an interesting question: how to establish a balance between the number of sensors to use and the number of times to sense? To address this question, we derive an optimal combination of these two design parameters that minimizes the overall sensing overhead. To our best knowledge, this is the first study to examine the impact of sensor mobility on the performance of spectrum sensing.

The performance gains, achieved by collaborative spectrum sensing in CRNs are well established in literature. The centralized collaborative spectrum sensing has been included in the IEEE 802.22 standard draft **??**1]. The secondary users report sensing results to a base station (fusion center) on a periodic or on-demand basis about the presence and absence of primary user using spectrum sensing. The secondary user trust is critical for such a cooperative systems to operate reliably. Trust-based mechanisms have been widely suggested for collaborative spectrum sensing under report falsifying attacks, where dishonest attackers lie on their sensing results.

The calculation of the trust of secondary users has been addressed using different techniques in the literature. The trust values can be calculated from the reports received from the secondary users, comparing deviation suffered by each from average [4]. The secondary users are penalized according to the deviations calculated. In another paper by the same authors [8], outlier techniques are studied in detail and based on the knowledge of partial primary user activity, malicious user(s) identification is done. Among other techniques, the Bayesian rule can be applied to compute the a posteriori probability of being an attacker for each secondary user. When the posteriori probability of a certain secondary user exceeds the suspicious level threshold, it is claimed to be an attacker and is removed from the collaboration [6]. For multiple attackers, the large number of combinations of attackers and honest users is removed by using an onion-peeling based approximation to reduce computational complexity.

Abnormality detection algorithm based on proximity, which is widely used in the field of data mining has been introduced in [3], to solve the problem of malicious users in the system using history reports of each secondary user. The proposed architecture in [7], needs to collect spectrum sensing data from multiple sources or equipment on consumer premises. This process is known as crowd sourcing. In [7], the area of interest is divided in to cells and the credibility of these devices are kept in check by corroboration among neighboring cells in a hierarchical structure to identify cells with significant number of malicious nodes.

In the solution proposed by authors in [5], focus is on a small region for enhancing the primary user detection by exploring the spatial diversity in user reports. In another paper by the same authors, [2], impact of mobility in spectrum sensing is analyzed. The authors show that because of mobility, the secondary user sensing results get uncorrelated faster thus giving better performance compared to spectrum sensing performed by static secondary users.

To the best of our knowledge, none of the existing work studied the impact of mobility on the malicious user detection and primary user detection under attack in CRNs. None of the existing trust-based collaborative spectrum sensing solutions are directly applicable for mobile scenarios, either. Our proposed solutions [13] are different from all the existing solutions that we separate the location reliability from the user trust, thus achieve better performance on malicious user detection which in turn improve the primary user detection under attacks in mobile scenarios.

Collaborative spectrum sensing is a key technology in cognitive radio networks (CRNs). Although mobility is an inherent property of wireless networks, there has been no prior work studying the performance of collaborative spectrum sensing under attacks in mobile CRNs. Existing solutions based on user trust for secure collaborative spectrum sensing cannot be applied to mobile scenarios, since they do not consider the location diversity of the network, thus over penalize honest users who are at bad locations with severe pathloss. In this paper, we propose to use two trust parameters, location reliability and malicious intention (LRMI), to improve both malicious user detection and primary user detection in mobile CRNs under attack. Location reliability reflects path-loss characteristics of the wireless channel and malicious intention captures the true intention of secondary users, respectively. We propose a primary user detection method based on location reliability (LR) and a malicious user detection method based on LR and Dempster-Shafer (D-S) theory.

8 Global Journal of Computer Science and Technology

Volume XIV Issue V Version I Year 2014 E Simulations show that mobility helps train location reliability and detect malicious users based on our methods. Our proposed detection mechanisms based on LRMI significantly outperforms existing solutions. In comparison to the existing solutions, we show an improvement of malicious user detection rate by 3 times and primary user detection rate by 20% at false alarm rate of 5%, respectively. Shraboni Jana et al [84] studied the performance of spectrum sensing under different pathloss and fading conditions and came up with a solution fitting for mobile CRNs. The numerically simulated results showed that our approach (LRMI) greatly improves malicious detection in mobile CRNs and hence, performance of collaborative-spectrum sensing for primary user detection. Thus mobile CRNs, need to be evaluated considering both the location from where the report was generated and who has generated the report. Mobility is also found to be an aiding factor in malicious users detection. The simulation results also show that as the average velocity of the secondary users in the system increases, the ROC curves for the system improves.

An interesting extension of the work will be to evaluate how malicious users can exploit mobility to their advantage and avoid getting detected. The primary user is static in our current model.

9 e) Spectrum Sensing Technique for Cognitive Radio Networks Under Denial of Service Attack

Jamming in wireless networks has been extensively studied. Most prior research assumes that the jammer is an external entity, oblivious to the protocol specifics and cryptographic secrets [25].Recently, several works have considered the problem of jamming by an internal adversary, who exploits knowledge of network protocols and secrets to launch DoS attacks on layers above the physical layer [13], [4], [7], [68], [6]. In this section, we classify related work based on the adversarial model.

Opportunistic spectrum access in CRNs makes them an easy target for attackers that may jeopardize its operation for their individual gains or merely because of malicious intent. Therefore, security of DSA in CRNs has been the focus of attention for many research efforts lately. This section provides an overview of related work and provides an insight as to how these studies differ from the work presented in this paper.

Measures to prevent the jamming of Common Control Channel (CCC) in an ad hoc CRN are presented in [69]. It assumes that the jammers are aware of the protocol specifics as well as cryptographic quantities used to secure network operations. The authors propose two techniques to identify malicious nodes that act independently and those that collude to jam the CCC. They also propose generation and secure elude jammers. This however is primarily aimed at defending against jamming the CCC through which spectrum sensing and other control data are shared. On the other hand, our work addresses defense against jamming of spectrum sensing itself.

In [1], authors consider an ad hoc CRN in which they introduce various types of jammers: jammers that jam a fixed channel, a random selection of channels and channels that are predicted to be used next in subsequent time slots. An algorithm is proposed with which senders and receivers learn the jammers' channel access pattern and can evade jamming by hopping to jamming-free channels. Our proposed DS3 algorithm does not resort to channel hopping and evades jamming while staying on the same channel.

A collaborative defense technique is presented in [2] where the SUs in a CRN defend against a collaborative DoS attack launched by sweeping and jamming the channels in the entire spectrum. The SUs make use of spatial and temporal diversity to form proxies in order to continue communicating. This work however does not consider that the jammer may seek to conserve its jamming power budget and jam only the fast sensing stage and the main defense against jamming attack is for the CRN to hop to another channel. Authors in [13] present a game theoretic approach to defend against jamming attacks in CRNS. They derive an optimal strategy for the SUs to decide whether to remain in the current band or to hop to another band by employing a Markov Decision Process approach. The authors propose a learning process through which SUs estimate current network conditions based on past observations using the maximum likelihood estimation technique. This work also does not consider the two-stage spectrum sensing that is employed in the current IEEE 802.22 WRAN draft standard, and the defense against jamming is for CRN to hop to another channel.

To the best of our knowledge, this is the first attempt to address a smart jamming attack by malicious users and to make maximum utilization of spectrum opportunities while staying in the spectrum band that is being jammed and not hopping away from it.

Cliff C. Zou et al [85] proposed a novel algorithm DS3, which minimizes the effects of smart jamming as well as noise on the fast sensing phase of DSA and improves spectrum utilization through dynamic fine sensing decision algorithm with minimal increase in the overhead caused due to additional delay in the detection of PU's presence on the spectrum. DS3 achieves up to 90% improvement in spectrum utilization under jamming attack while keeping the PU detection delay to less than 50% of the maximum allowed PU detection delay. The collaborative or cooperative spectrum sensing paradigm in CRN opens a way to the attackers who can falsify the sensing results. The motivation of an attacker can be either selfish or malicious. Being selfish, an attacker may report the presence of the primary user when there is actually none in order to deny the legitimate users' access to the spectrum (Denial of Service attack). While being malicious, an attacker may report an absence of the primary user when there is one, thus causing chaos and interference for primary and secondary users. Here in this paper we explored the contemporary affirmation of the recent literature on secure spectrum sensing, which indicates the opportunity for significant research to devise novel cooperation and collaboration strategies for CRNs, which are in regard to blocking the vulnerabilities that let the falsification of the cooperation and collaboration.

10 Global Journal of Computer Science and Technology

Volume XIV Issue V Version I Year 2014 [1]

1

Figure 1: Figure 1 :

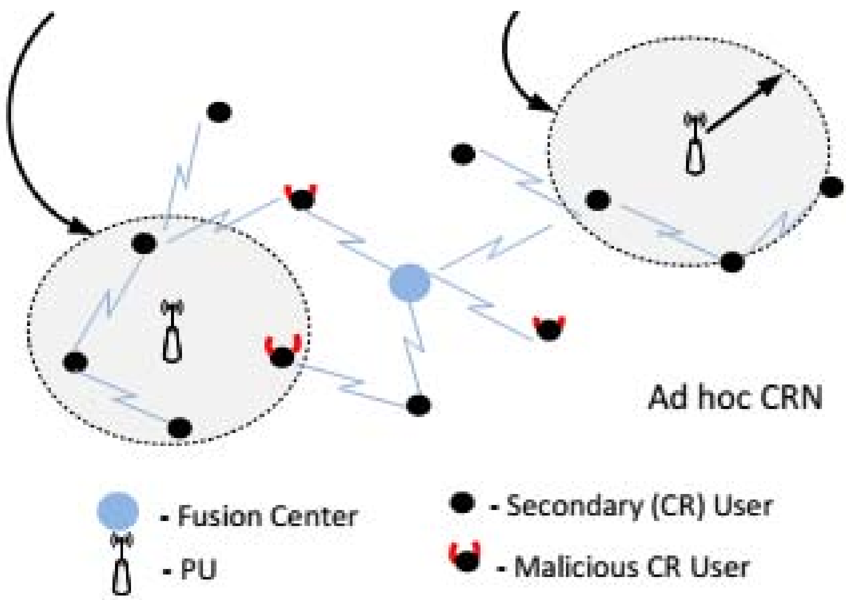

Figure 2:

[Jana and Zeng] , S Jana , ; Kai Zeng .

[Cheng] , Wei Cheng .

[Somasundaram and Subbalakshmi (2003)] '3-D Multiple Description Video Coding for Packet Switched Networks'. S Somasundaram , K P Subbalakshmi . *Proceedings of the IEEE International Confer¬ence on Multimedia and Expo*, (the IEEE International Confer¬ence on Multimedia and ExpoBaltimore) 6-9 July 2003. p. .

[Olivieri et al. (2005)] 'A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrallyagile software defined radios'. M P Olivieri , G Barnett , A Lackpour , A Davis , P Ngo . *Proc. DySPAN*, (DySPAN) Nov. 2005. p. .

[Yucek and Arslan ; Qin ()] 'A survey of spectrum sensing algorithms forcognitive radio applications'. T Yucek , H Arslan ; Qin , T . *SIGMOBILE Mobile Computational Communication Reviews* 2009. 12 p. . (Towards a trust aware cognitive radio architecture)

[Zhang et al. (2006)] 'A Trust Based Framework forSecure Data Aggregation in Wireless Sensor Networks'. W Zhang , S K Das , Y Liu . *Proc.IEEE Third Ann. Comm. Soc. Conf. Sensor and Ad Hoc Comm. andNetworks (SECON '06)*, (.IEEE Third Ann. Comm. Soc. Conf. Sensor and Ad Hoc Comm. andNetworks (SECON '06)) Sept. 2006.

[Du et al. (2003)] 'A Witness-BasedApproach for Data Fusion Assurance in Wireless Sensor Networks'. W Du , J Deng , Y S Han , P K Varshney . *Proc. IEEE Global Telecomm. Conf. (GlobeCom '03)*, (IEEE Global Telecomm. Conf. (GlobeCom '03)) Dec.2003.

[Beibeiwang and Rayliu2011] 'AdvancesinRadio CognitiveNetworks:ASurvey'. K J Beibeiwang , Rayliu2011 . *IEEEJournalof selected topics in Signal Processing*, 5.

[Akyildiz et al. ()] I F Akyildiz , W.-Y Lee , K R Chowdhury . *CRAHNs: cognitive radioad hoc networks*, 2009. 7 p. .

[Liu et al. ()] 'Aldo: An anomaly detection framework for dynamic spectrum accessnetworks'. S Liu , Y Chen , W Trappe , L J Greenstein . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2009.

[Amjad et al.] M F Amjad , B Aslam , C C Zou . *Reputation Aware Collaborative Spectrum Sensing for Mobile*,

[Anand et al. ()] 'An Analytical Modelfor Primary User Emulation Attacks in Cognitive Radio Networks'. S Anand , Z Jin , K P Subbalakshmi . *Proc. IEEE Symp Communications Surveys Tutorials*, (IEEE Symp Communications Surveys Tutorials) 2009. 11 p. .

[Cheng et al. ()] 'An Efficient Spectrum Sensing Scheme for Cognitive Radio'. S Cheng , V Stankovic , L Stankovic . *IEEE Signal Processing Letters* 2009. 16 (6) p. .

[Min and Shin] *An Optimal SensingFramework Based on Spatial RSS-profile in*, A W Min , K G Shin .

[Popper et al. ()] 'Anti jamming broadcast communication using uncoordinated spread spectrum techniques'. C Popper , M Strasser , S ?capkun . *IEEE Journal onSelected Areas in Communication* 2010. 28 (5) p. .

[Goenka and Raut ()] 'Application of Fountain Codes to Cognitive Radio Networks and MBMS-A Re-view'. K V Goenka , R D Raut . *International Journal of Computer Applications* 2013. 66 (14) p. .

[Duan et al. (2012)] 'Attack Prevention forCollaborative Spectrum Sensing in Cognitive Radio Networks'. L Duan , A Min , J Huang , K Shin . *IEEEJournal on Seleted Areas in Communications* Oct. 2012. 30 (9) p. .

[Min et al. (2009)] 'Attack-tolerant distributed sensingfor dynamic spectrum access networks'. A W Min , K G Shin , X Hu . *Proc. ICNP*, (ICNP) Oct. 2009.

[Byers et al. (2013)] J W Byers , M Luby , M Mitzenmacher , A Rege . *A Digital Fountain Approach to Reliable Network Security (CNS), 2013 IEEE Conference on*, Oct. 2013. 27 p. .

[Wang et al. (2009)] 'Catch it: Detect malicious nodesin collaborative spectrum sensing'. W Wang , H Li , Y Sun , Z Han . *Proc. IEEE Globecom*, (IEEE Globecom) Apr. 2009.

[Li and Han ()] 'Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitiveradio networks'. H Li , Z Han . *IEEE Transactions on Wireless Communications* 2010. 9 p. .

[Li and Han (2010)] 'Catching attacker(s) for collaborative spectrumsensing in cognitive radio systems: An abnormility detection approach'. H Li , Z Han . *Proc. IEEE DySPAN*, (IEEE DySPAN) Apr. 2010.

[Mishra et al. ()] 'Coexistencewithp rimaryusers of different scales'. S M Mishra , R Tandra , Sahai . *inProc. IEEE Dynamic Spectrum AccessNetworks (DySPAN)* 2007.

[Pawelczak et al. (2005)] 'Cognitive radio emergency networks -requirements and design'. P Pawelczak , R V Prasad , X Liang Xia , I G M M Niemegeers . *Proc. DySPAN*, (DySPAN) Nov. 2005. p. .

[Haykin ()] 'Cognitive Radio: Brain-Empowered Wireless Communications'. S Haykin . 10.1109/JSAC.2004.839380. *IEEE Journal on Selected Areas Com-munications* 2005. 23 (2) p. .

[CognitiveRadio Networks Proc. IEEE SECON '09 ()] 'CognitiveRadio Networks'. *Proc. IEEE SECON '09*, (IEEE SECON '09) June2009.

[Wenjing et al. ()] 'Collaborative jamming and collaborative defense in Cognitive Radio Networks'. W Wenjing , M Chatterjee , K Kwiat . *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2011.

[Mody (2008)] *Collaborative Sensing for Security*, A Mody . IEEE 802.22-08/0301r011. Dec. 2008.

[Ghasemi and Sousa (2005)] 'Collaborative Spectrum Sensing for Opportunistic Access in Fading Environ-ments'. A Ghasemi , E S Sousa . *Proceedings of IEEE International Symposium on New Frontier in Dynamic Spectrum Access Network*, (IEEE International Symposium on New Frontier in Dynamic Spectrum Access NetworkBaltimore) 8-11 November 2005. p. .

[Nosratinia et al. ()] 'Cooperative communication in wireless network'. A Nosratinia , T E Hunter , A Hedayat . 10.1109/MC0M.2004.1341264. *IEEE Communica-tionsMagazine* 2004. 42 (10) p. .

[Ganesan and Li (2005)] 'Cooperative Spectrum Sensing in Cognitive Radio Networks'. G Ganesan , Y Li . *Proceedings of IEEE Inter-national Symposium on New Frontier in Dynamic Spec-trum Access Network*, (IEEE Inter-national Symposium on New Frontier in Dynamic Spec-trum Access NetworkBaltimore) 8-11 November 2005. p. .

[Woyach et al. (2008)] 'Crime andPunishment for Cognitive Radios'. K A Woyach , A Sahai , G Atia , V Saligrama . *Proc. IEEE 46th Ann. AllertonConf. Comm., Control and Computing*, (IEEE 46th Ann. AllertonConf. Comm., Control and Computing) Sept. 2008.

[Zhao et al. (2005)] 'Decentralized cognitive mac for dynamic spectrum access'. Q Zhao , L Tong , A Swami . *Proc. DySPAN*, (DySPAN) Nov. 2005. p. .

[Chen et al. (2008)] 'Defense against Primary UserEmulation Attacks in Cognitive Radio Networks'. R Chen , J.-M Park , J H Reed . *IEEE J. SelectedAreas in Comm* Jan. 2008. 26 (1) p. .

[Wild and Ramchandran (2005)] 'Detecting primary receivers for cognitive radio applications'. B Wild , K Ramchandran . *Proc. DySPAN*, (DySPAN) Nov. 2005. p. .

[Amjad et al. (2013)] 'DS3: A Dynamic and Smart Spectrum Sensing Technique for Cognitive Radio Networks Under Denial of Service Attack'. Faisal Amjad , Cliff C Baber Aslam , Zou . *Atlanta* Dec. 9-13, 2013. (to appear in IEEE Globecom)

[Zhao and Sadler ()] 'Dynamic Spectrum Access: Signal Processing, Networking, and Regulatory Policy'. Q Zhao , B M Sadler . *IEEE Signal Processing Magazine* 2006. 24 p. .

[Steadman et al. (2007)] 'Dynamic Spectrum Sharing Detectors'. K N Steadman , A D Rose , T T N Nguyen . *Proc. of IEEE International Symposium on New Frontiers in Dynamic SpectrumAccess Networks*, (of IEEE International Symposium on New Frontiers in Dynamic SpectrumAccess NetworksDublin, Ireland) DySPAN 2007. April 2007. p. .

[Urkowitz ()] 'Energy Detection of Unknown Determi-nistic Signals'. H Urkowitz . 10.1109/PRQC.1967.5573. *Proceedings of the IEEE* 1967. 55 (4) p. .

[Urkowitz (1967)] 'Energy detection of unknown deterministic signals'. H Urkowitz . *Proc. IEEE*, (IEEE) Apr. 1967. 55 p. .

[Facilitating Opportunities for Flexible, Efficient and Reliable Spectrum Use Employing Cognitive Radio Technologies", notice of *Facilitating Opportunities for Flexible, Efficient and Reliable Spectrum Use Employing Cognitive Radio Technologies", notice of proposed rulemaking and order*, FCC 03-322. December 2003. (Federal Communications Commission)

[FCC Spectrum Policy Task Force: Report of the spectrum efficiencyworking group (2002)] *FCC Spectrum Policy Task Force: Report of the spectrum efficiencyworking group*, November 2002. 2008. Genève. 39. (ITU Radio Regulations, International Telecommunication Union)

[Federal Communications Commission Spectrum Policy Task Force (2002)] *Federal Communications Commission Spectrum Policy Task Force*, November 2002. (Report of the Spectrum Efficiency Working Group)

[Mackay ()] 'Fountain Codes'. D J C Mackay . *IEEE Communica-tions* 2005. 152 (6) p. .

[Min and Shin ()] 'Impact of mobility on spectrum sensingin cognitive radio networks'. A W Min , K G Shin . *Proc. of the 2009 ACM workshop onCognitive radio networks*, (of the 2009 ACM workshop onCognitive radio networks) 2009.

[Liu et al. (2007)] 'Insider Attacker Detection inWireless Sensor Networks'. F Liu , X Cheng , D Chen . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) May 2007.

[Su et al. ()] 'Jamming-Resilient Dynamic Spectrum Access for Cognitive Radio Networks'. H Su , Q Wang , K Ren , K Xing . *IEEE International Conference on Communications (ICC)*, 2011.

[Strasser et al. ()] 'Jamming-resistant keyestablishment using uncoordinated frequency hopping'. M Strasser , C Popper , S Capkun , M Cagalj . *Proceedings of IEEE Symposium on Security and Privacy*, (IEEE Symposium on Security and Privacy) 2008.

[Luo and Hubaux ()] 'Joint Mobility and Routingfor Lifetime Elongation in Wireless Sensor Networks'. J Luo , J.-P Hubaux . *Proc. IEEE INFOCOM '05*, (IEEE INFOCOM '05) Mar2005. p. .

[Wellens and Mähönen (2009)] 'Lessons Learned from an Extensive Spectrum Occupancy Measurement Campaign and a Stochastic Duty Cycle Model'. M Wellens , P Mähönen . *Proc. of TridentCom*, (of TridentComWashington D.C., USA) 2009. April 2009. p. .

[Devroye et al. ()] 'Limits on Com-munications in a Cognitive Radio Channel'. N Devroye , P Mitran , V Tarokh . 10.1109/MC0M.2006.1668418. *IEEE Com-munications Magazine* 2006. 44 (6) p. .

[Luby (2002)] 'LT Codes'. M Luby . *Proceedings of the 43rd Annual Vancouver*, (the 43rd Annual Vancouver) November 2002. p. .

[Kaligineedi et al. (1998)] 'Malicious userdetection in a cognitive radio cooperative sensing system'. P Kaligineedi , M Khabbazian , V K Bhargava . *Proceedings of ACM SIGCOMM 98*, (ACM SIGCOMM 98) Aug. 2010. September 1998. Van¬couver. 9 p. . (Distribution of Bulk Data)

[Networks] *Military Communications*, Cognitive Radio Networks .

[Tague et al. ()] 'Mitigation of control channel jammingunder node capture attacks'. P Tague , M Li , R Poovendran . *IEEE Transactions on Mobile Computing* 2009. 8 (9) p. .

[Liu et al. (2005)] 'Mobility Improves Coverage of Sensor Networks. InProc'. B Liu , P Brass , O Dousse , P Nain , D Towsley . *ACM MobiHoc '05*, May 2005. p. .

[Akyildiz et al. ()] 'NeXt generation/dynamic spectrum access/cognitive radio wireless networks:a survey'. I F Akyildiz , W.-Y Lee , M C Vuran , S Mohanty . *Computer Networks* 2006. 50 (13) p. .

[Digham (2002)] 'On signal transmission and detection over fadingchannels'. F F Digham . *inProc.IEEE Int. Conf. Commun* Jul. 2005. 36. May 2002. p. . Univ. Minnesota (Ph.D. dissertation) (Energy detection of a signal with random amplitude)

[Digham et al. (2003)] 'On the Energy Detection of Unknown Signals over Fading Chan-nels'. F Digham , M.-S Alouini , M K Simon . *IEEE Transactions on Communictions* May 2003. p. .

[Lopez-Benitez and Casadevall (2010)] 'On the Spectrum Occupancy Perception of Cognitive Radio Terminals in Realistic Scenarios'. M Lopez-Benitez , F Casadevall . *International Workshop on Cognitive Information Processing*, (Elba) June 2010. p. .

[Wu et al.] 'Optimal Defense against Jamming Attacks in Cognitive Radio Networks Using the Markov Decision Process Approach'. Y Wu , B Wang , K J R Liu . *IEEE Global Telecommunications Conference (GLOBECOM)*, p. 2010.

[Tague et al. ()] 'Probabilistic mitigation of controlchannel jamming via random key distribution'. P Tague , M Li , R Poovendran . *Proceedings of PIRMC*, (PIRMC) 2007.

[Liu et al. ()] 'Randomized differential DSSS:Jamming-resistant wireless broadcast communication'. Y Liu , P Ning , H Dai , A Liu . *Proceedings ofthe INFOCOM*, (the INFOCOM) 2010.

[Chen et al. ()] 'Robust distributed spectrum sensing in cognitive radio networks'. R Chen , J M Park , K Bian . *Proc. IEEE INFOCOM*, (IEEE INFOCOM) 2008.

[Wang and Zheng (2006)] 'Route and spectrum selection in dynamic spectrum networks'. Q Wang , H Zheng . *Proc. CCNC*, (CCNC) Jan. 2006. p. .

[Yang et al. (2006)] 'SDAP: A Secure Hop-byHop Data Aggregation Protocol for Sensor Networks'. Y Yang , X Wang , S Zhu , G Cao . *Proc. ACM Mobi Hoc*, (ACM Mobi Hoc) May 2006.

[Kushwaha and Chandramouli ()] 'Secondary Spec¬trum Access with LT Codes for Delay Constrained Applications'. H Kushwaha , R Chandramouli . *Proceedings of the IEEE Consumer Commu-nications and Networking Conference*, (the IEEE Consumer Commu-nications and Networking ConferenceLas Vegas, Janu¬ary) 2007. p. .

[Fatemieh et al. (2010)] *Secure collaborativesensing for crowdsourcing spectrum data in white space networks*, O Fatemieh , R Chandra , C A Gunter . Apr. 2010. (inProc. IEEE DySPAN)

[Min et al. (2008)] 'Secure Cooperative Sensing in IEEE802.22 WRANs Using Shadow Fading Correlation'. A Min , K Shin , X Hu . *IEEETransactionson Mobile Computing* Apr. 2008. 10 (10) p. .

[Choi; Shin (2013)] 'Secure cooperative spectrum sensing in cognitive radio networks using interference signatures'. Seunghyun Choi; Shin , KG . *MILCOM 2013 -2013 IEEE*, 18-20 Nov. 2013. 956 p. 951.

[Kaligineedi et al. (2008)] 'Secure cooperativesensing techniques for cognitive radio systems'. P Kaligineedi , M Khabbazian , V K Bhargava . *Proc. ICC*, (ICC) Sep. 2008.

[Proa? and Lazos ()] 'Selective jamming attacks in wireless networks'. A Proa? , L Lazos . *Proceedings of ICC*, (ICC) 2010.

[Liang et al. ()] 'Sensing-Throughput Tradeoff for Cognitive RadioNetworks'. Y.-C Liang , Y Zeng , E C Y Peh , A T Hoang . *IEEE Transactions on WirelessCommunications* 2008. 7 p. .

[Ma et al. ()] 'Signal processing in cognitive radio'. J Ma , G Li , B H Juang . *Proceedings of the IEEE* 2009. 97 (5) p. .

[Simon et al. ()] M K Simon , J K Omura , R A Scholtz , B K Levitt . *Spread SpectrumCommunications Handbook*, 2001. McGraw-Hill.

[Challapali et al. (2004)] 'Spectrum agile radio: Detecting spectrum opportunities'. K Challapali , S Mangold , Z Zhong . *Proc.6th Annual Int'l Symposium on Advanced Radio Technologies*, (.6th Annual Int'l Symposium on Advanced Radio Technologies) March 2004.

[Etkin et al. ()] 'Spectrum Sharing for Unlicensed Bands'. R Etkin , A Parekh , D Tse . *IEEE Journal on Selected Areas in Communications* 2005. 25 (3) p. .

[Valenta et al. (2010)] 'Survey on Spectrum Utilisation in Europe: Measurements, Analysis and Observations'. V Valenta , R Mar?alek , G Baudoin , M Villegas , M Suarez , F Robert . *Proc. of ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, (of ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)Cannes, France) June 2010. p. .

[Liu et al. (1558)] 'Thwarting Control-Channel Jamming Attacks from Inside Jammers'. S Liu , L Lazos , M Krunz . *IEEE Transactions on Mobile Computing* 1558. Sept. 2012. 11 (9) p. 1545.

[Hosseini and Falahati ()] 'Transmission over Cognitive Radio Channel with Novel Secure LT Code'. E Hosseini , A Falahati . 10.4236/cn.2013.53023. *Communications and Network* 2013. 5 (3) p. .

[Jana ()] 'Trusted collaborative spectrum sensing for mobile cognitive radio networks'. S Jana . *32nd IEEE International Conference on Computer Communications, INFOCOM*, 2012.

[Mohapatra (2013)] 'Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks'. P Mohapatra . *IEEE Transactions on* Sept. 2013. 8 (9) p. . (Information Forensics and Security)

[Wei ()] 'Two-TierOptimal Cooperation Based Secure Distributed Spectrum Sensing for Wireless Cognitive Radio Networks'. Jin Wei . *IEEE INFOCOM* 2010.

[Peng et al.] *Utilization and Fairness in Spectrum Assignment for Opportunistic Spectrum Access*, C Peng , H Zheng , B Y Zhao . ACM Monet. (to appear)

[WRAN WG onBroadband Wireless Access Standards] Available: IEEE 802.22. *WRAN WG onBroadband Wireless Access Standards*,